

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES ARMÉES

Arrêté du 27 août 2025 portant approbation de l'instruction ministérielle n° 900 relative à la protection de l'information et des données

NOR : ARMM2525751A

Le ministre des armées,

Vu le code de la défense, notamment ses articles R. 2311-1 à R. 2311-9-1 ;

Vu le code pénal, notamment son article 413-9 ;

Vu l'arrêté du 29 novembre 2011 portant création de traitements automatisés de données à caractère personnel relatifs à la gestion des habilitations au secret de la défense nationale ;

Vu l'arrêté du 21 mars 2012 modifié portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale ;

Vu l'arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale,

Arrête :

Art. 1^{er}. – L'instruction ministérielle n° 900 relative à la protection de l'information et des données annexée au présent arrêté est approuvée.

Art. 2. – Le présent arrêté entre en vigueur le 1^{er} novembre 2025.

Art. 3. – L'arrêté du 15 mars 2021 portant approbation de l'instruction ministérielle n° 900 sur la protection du secret et des informations diffusion restreinte et sensibles est abrogé.

Art. 4. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 27 août 2025.

SÉBASTIEN LECORNU



ANNEXE

INSTRUCTION MINISTÉRIELLE N° 900/ARM/CAB du 27 août 2025

RELATIVE À LA PROTECTION DE L'INFORMATION ET DES DONNÉES

Abroge et remplace l'instruction ministérielle
N° 900/DEF/CAB/NP du 15 mars 2021

TABLE DES MATIÈRES

TITRE 1 : PRINCIPES GÉNÉRAUX.....	1
TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE	7
INTRODUCTION : CHAÎNES FONCTIONNELLES DE LA PROTECTION DU SECRET	7
2.1 : FONCTIONNAIRE DE SÉCURITÉ DE DÉFENSE ET FONCTIONNAIRE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION	10
2.2 : SERVICES ENQUÊTEURS DU MINISTÈRE DE LA DÉFENSE	12
2.3 : AUTORITÉS D'HABILITATION DU MINISTÈRE DE LA DÉFENSE.....	15
2.4 : RESPONSABILITÉS DU RESPONSABLE D'ORGANISME	17
2.5 : OFFICIER DE SÉCURITÉ	19
2.6 : OFFICIER DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DES PERSONNES MORALES LIÉES PAR CONTRAT OU CONVENTION AVEC LE MINISTÈRE DE LA DÉFENSE	27
2.7 : BUREAU DE PROTECTION DU SECRET	31
2.8 : FORMATION ET SENSIBILISATION	34
2.9 : INSPECTIONS, AUDITS ET CONTRÔLES DES PERSONNES MORALES DÉTENANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS ET DES SYSTÈMES NUMÉRIQUES NÉCESSAIRES À L'EXÉCUTION DU CONTRAT	39
TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES	43
INTRODUCTION : PROCESSUS D'HABILITATION DU PERSONNEL	43
3.1 : CATALOGUE DES EMPLOIS	44
3.2 : DEMANDE D'HABILITATION	46
3.3 : AVIS DE SÉCURITÉ	50
3.4 : MISE EN ÉVEIL ET MISE EN GARDE	53
3.5 : DÉCISION D'HABILITATION OU DE REFUS D'HABILITATION	55
3.6 : GESTION ET FIN DE L'HABILITATION	58
3.7 : CAS DES HABILITATIONS OTAN ET UE	62
3.8 : CONTRÔLE DES RESSORTISSANTS ÉTRANGERS EN CAS D'HABILITATION OU D'ACCÈS A DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS OU CONTENANT DES INFORMATIONS <i>DIFFUSION RESTREINTE</i> OU SENSIBLES	65
3.9 : ENQUÊTES ADMINISTRATIVES POUR LE RENSEIGNEMENT ET LA SÛRETÉ	68
3.10 : OBLIGATION DE RÉSERVE, DISCRÉTION PROFESSIONNELLE ET SECRET PROFESSIONNEL POUR LES AGENTS DU MINISTÈRE DE LA DÉFENSE	77
3.11 : PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL COMPORTANT LA MENTION DE LA QUALITÉ DE MILITAIRE	80
TITRE 4 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS.....	86
INTRODUCTION : PRINCIPES GÉNÉRAUX DE LA PROTECTION DU SECRET ET DE SÉCURITÉ NUMÉRIQUE DANS LES CONTRATS	86
4.1 : ACTEURS DES CONTRATS.....	90
4.2 : CHOIX DU TYPE DE CONTRAT.....	96
4.3 : MODALITÉS DE PASSATION D'UN CONTRAT SENSIBLE	99
4.4 : PRISE EN COMPTE DE LA PROTECTION DU SECRET DANS LA PROCÉDURE D'ACHAT	101
4.5 : PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS : SÉLECTION DES CANDIDATS ADMIS À SOUMISSIIONNER ET CONTENU DES OFFRES	103
4.6 : PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS : CONSULTATION DES INFORMATIONS ET SUPPORTS CLASSIFIÉS DURANT LA PÉRIODE D'ÉLABORATION DES OFFRES.....	106

4.7 : PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS :.....	109
EXAMEN DES OFFRES, CHOIX DE L'ATTRIBUTAIRE ET SIGNATURE	109
4.8 : PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS : PLAN CONTRACTUEL DE SÉCURITÉ.....	113
4.9 : CAS D'UNE PERSONNE MORALE ÉTRANGÈRE CANDIDATE À LA PASSATION D'UN CONTRAT IMPLIQUANT L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS	118
4.10 : HABILITATION INITIALE DE LA PERSONNE MORALE	120
4.11 : GESTION ET FIN DE L'HABILITATION DE LA PERSONNE MORALE.....	124
4.12 : GESTION DES SOUS-CONTRACTANTS DANS LES CONTRATS AVEC ACCÈS OU DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS	126
4.13 : CONTRÔLES DES PERSONNES MORALES PAR LES AUTORITÉS CONTRACTANTES, LES AUTORITÉS D'HABILITATION, L'AUTORITÉ DE SÉCURITÉ DÉLÉGUÉE ET LE SERVICE ENQUÊTEUR.....	128

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS 131

INTRODUCTION : NORMES DE PROTECTION PHYSIQUE ET LOGIQUE APPLICABLES AUX INFORMATIONS ET SUPPORTS CLASSIFIÉS	131
5.1 : ZONE PROTÉGÉE	144
5.2 : ZONE RÉSERVÉE.....	149
5.3 : ÉLÉMENTS CLASSIFIÉS CONSERVÉS HORS COFFRE	153
5.4 : ACTIVITÉS NÉCESSITANT L'ACCÈS À DES INFORMATIONS ET SUPPORTS CLASSIFIÉS EN DEHORS DE LEUR LIEU ABRITANT	157
5.5 : MATÉRIEL D'IMPRESSION, DE REPRODUCTION ET DE DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIÉS.....	160
5.6 : PROTECTION CONTRE LES COMPROMISSIONS VIA LES ÉQUIPEMENTS ÉLECTRONIQUES	162
5.7 : CONTRÔLES D'APTITUDE PHYSIQUE À LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS	165
5.8 : ACCÈS DE PERSONNES NON QUALIFIÉES AUX LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS	170
5.9 : ACCÈS DES MAGISTRATS AUX INFORMATIONS ET SUPPORTS CLASSIFIÉS	173

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ 176

INTRODUCTION : REMARQUES GÉNÉRALES	176
6.1 : CARTOGRAPHIE DES SYSTÈMES D'INFORMATION DES PERSONNES MORALES DE DROIT PRIVÉ CONTRACTANTES	177
6.2 : LE PROCESSUS D'HOMOLOGATION	179
6.3 : CONTRÔLE D'APTITUDE AU TRAITEMENT D'INFORMATIONS NUMÉRIQUES CLASSIFIÉES	187
6.4 : LES AUDITS DE SÉCURITÉ.....	190
6.5 : SOUS-CONTRACTANCE À UN TIERS EN MATIÈRE INFORMATIQUE	193
6.6 : PRISE EN COMPTE DE LA SÉCURITÉ DANS LE CYCLE DE VIE DES SYSTÈMES NUMÉRIQUES	196
6.7 : ÉQUIPEMENTS MOBILES ET SUPPORTS AMOVIBLES.....	201
6.8 : SUPERVISION DE SÉCURITÉ D'UN SYSTÈME NUMÉRIQUE	204
6.9 : LES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ACSSI). 206	
6.10 : SÉCURITÉ DU CÂBLAGE ET CIRCUITS APPROUVÉS	211

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET DES DONNÉES TOUT AU LONG DE LEUR CYCLE DE VIE..... 213

INTRODUCTION : PRINCIPES ET DÉFINITIONS	213
7.1 : ÉLABORATION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS	216
7.2 : MENTION DE PROTECTION <i>DIFFUSION RESTREINTE</i>	221
7.3 : MENTION COMPLÉMENTAIRE DE PROTECTION <i>SPECIAL FRANCE</i>	225
7.4 : MENTION COMPLÉMENTAIRE DE PROTECTION COMMUNICABLE À [SERVICES, ÉTATS, ORGANISATIONS INTERNATIONALES, INSTITUTIONS, ORGANES OU ORGANISMES DE L'UE]	227
7.5 : MENTIONS DE CONFIDENTIALITÉ SPÉCIFIQUES	229
7.6 : CAS PARTICULIER DES INFORMATIONS ET SUPPORTS CLASSIFIÉS <i>TRES SECRET</i> CLASSIFICATION SPÉCIALE	235
7.7 : ENREGISTREMENT ET INVENTAIRE.....	236
7.8 : DIFFUSION ET TRANSPORT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS.....	240
7.9 : IMPRESSION/REPRODUCTION DES INFORMATIONS CLASSIFIÉES	248
7.10 : STOCKAGE DES INFORMATIONS ET SUPPORTS CLASSIFIÉS.....	250
7.11 : VERSEMENT DANS UN SERVICE D'ARCHIVES	252
7.12 : DÉCLASSIFICATION OU DECLASSERMENT D'UNE INFORMATION CLASSIFIÉE	254
7.13 : DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIÉS, <i>DIFFUSION RESTREINTE</i> OU SENSIBLES	261
7.14 : ÉVACUATION ET DESTRUCTION D'URGENCE	264

TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA DÉFENSE NATIONALE266

INTRODUCTION : GÉNÉRALITES	266
8.1 : TRAITEMENT DES COMPROMISSIONS	268
8.2 : COMPROMISSION AFFECTANT UN SYSTÈME NUMÉRIQUE	272
8.3 : COMPROMISSION D'INFORMATIONS CLASSIFIÉES ÉTRANGÈRES	274

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES276

INTRODUCTION : PRINCIPES DE LA PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES.....	276
9.1 : AUTORITÉ NATIONALE DE SÉCURITÉ ET AUTORITÉ DE SÉCURITÉ DÉLÉGUÉE	277
9.2 : CONDITIONS POUR ÉCHANGER DES INFORMATIONS ET SUPPORTS CLASSIFIÉS AVEC L'ÉTRANGER	280
9.3 : CAS SPÉCIFIQUE DES CONTRATS INTERNATIONAUX : PLAN CONTRACTUEL DE SÉCURITÉ INTERNATIONAL (PCSI)	284
9.4 : ÉCHANGES NUMÉRIQUES CLASSIFIÉS AVEC L'ÉTRANGER	287
9.5 : MISSIONS ET SEJOURS À L'ÉTRANGER.....	288

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION292

INTRODUCTION : GÉNÉRALITÉS	292
10.1 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE.....	295
10.2 : MESURES APPLICABLES AUX PERSONNES PHYSIQUES.....	297
10.3 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS À L'ÉTRANGER ET EN OPÉRATION	300
10.4 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS	303
10.5 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA DÉFENSE NATIONALE	305

ANNEXES.....	307
ANNEXE 1 : LISTE DE EMPLOIS SENSIBLES	308
ANNEXE 2 : DÉCISION D'HABILITATION (PERSONNEL CIVIL)	309
ANNEXE 3 : DÉCISION D'HABILITATION (PERSONNEL MILITAIRE)	310
ANNEXE 4 : ENGAGEMENT DE RESPONSABILITÉ.....	311
ANNEXE 5 : DÉCISION DE REFUS D'HABILITATION (PERSONNEL CIVIL).....	312
ANNEXE 6 : DÉCISION DE REFUS D'HABILITATION (PERSONNEL MILITAIRE)	313
ANNEXE 7 : RÉCEPISSÉ DE NOTIFICATION D'UNE DÉCISION DE REFUS D'HABILITATION OU D'ABROGATION D'UNE DÉCISION D'HABILITATION (PERSONNEL CIVIL).....	314
ANNEXE 8 : RÉCEPISSÉ DE NOTIFICATION D'UNE DÉCISION DE REFUS D'HABILITATION OU D'ABROGATION D'UNE DÉCISION D'HABILITATION (PERSONNEL MILITAIRE)	315
ANNEXE 9 : DÉCISION D'ACCÈS AUX INFORMATIONS ET SUPPORTS CLASSIFIÉS POUR L'HABILITATION D'UNE PERSONNE PHYSIQUE DANS LE CADRE D'UN CONTRAT OU D'UNE CONVENTION AVEC LE MINISTÈRE DE LA DÉFENSE	316
ANNEXE 10 : DÉCISION DE CRÉATION DE ZONE RESERVÉE	317
ANNEXE 11 : LISTE DES PIÈCES CONSTITUTIVES DU DOSSIER TECHNIQUE D'APTITUDE PHYSIQUE D'UN ÉTABLISSEMENT POUR L'EXÉCUTION D'UN CONTRAT IMPLIQUANT LA DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS	318
ANNEXE 12 : RECOMMANDATIONS POUR LA MISE EN ŒUVRE ET LE FONCTIONNEMENT D'UN POSTE (CENTRAL) DE SÉCURITÉ D'UNE PERSONNE MORALE SOUS CONTRAT OU CONVENTION AVEC LE MINISTÈRE DE LA DÉFENSE	319
ANNEXE 13 : GUIDE LIÉ AUX CONDITIONS D'EMPLOI DES NIVEAUX DE CLASSIFICATION <i>SECRET ET TRES SECRET</i>	322
ANNEXE 14 : ENGAGEMENT DE NON-DIVULGATION DES INFORMATIONS ET SUPPORTS <i>DIFFUSION RESTREINTE</i>	332
ANNEXE 15 : FICHE DE POSITION	333
ANNEXE 16 : CAHIER D'ENREGISTREMENT DU COURRIER CLASSIFIÉ	334
ANNEXE 17 : INVENTAIRE CONTRADICTOIRE.....	336
ANNEXE 18 : DEMANDE DE DESTRUCTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS <i>TRES SECRET</i>	337
ANNEXE 19 : MESURES CONSERVATOIRES ET CONDUITE À TENIR EN CAS DE COMPROMISSION POSSIBLE AFFECTANT UN SYSTÈME NUMÉRIQUE	338
ANNEXE 20 : DOCUMENTS TRAITANT D'INFORMATIONS ET SUPPORTS CLASSIFIÉS À L'INTERNATIONAL	339
ANNEXE 21 : DURÉE ET MODALITÉS DE CONSERVATION DES DOCUMENTS DE GESTION EN PROTECTION DU SECRET.....	348
ANNEXE 22 : CATÉGORISATION DES SYSTÈMES NUMÉRIQUES	351
ANNEXE 23 : LE DOSSIER DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (DSSI).....	352

TITRE 1 : PRINCIPES GÉNÉRAUX**1****Références :**

- Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), notamment ses articles 2, 23, 24, 30 et 33
- Code du patrimoine – articles L.212-2, L.212-3, L.213-1 et suivants
- Code de la sécurité intérieure – article L.114-1 et suivants
- Code des relations entre le public et l'administration – articles L.311-5 et L.311-6
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 6, 31, 58, 115 et suivants
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment son article 85 et ses articles 140 et suivants
- Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique
- Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (IGI 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale)
- Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics
- Instruction générale interministérielle (IGI) n° 2102 sur la protection en France des informations classifiées de l'Union européenne (UE)
- Instruction interministérielle (II) n° 2100 pour l'application en France du système de sécurité de l'Organisation du Traité de l'atlantique nord (OTAN)
- Instruction ARM/SGA/DAJ/D2P/DPSP du 31 janvier 2020 relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense

Points clés

- La présente instruction décline la politique de protection du secret de la défense nationale et celle de sécurité numérique en modalités d'application, constituant ainsi une politique globale de protection de l'information et des données pour le périmètre du ministère de la défense.
- Cette instruction intègre également des dispositions relatives à la protection des informations et supports qui, sans être classifiés ou protégés par la mention *Diffusion Restreinte*, sont considérées comme sensibles au ministère.
- Au sein du ministère de la défense, la sécurité numérique participe à la

TITRE 1 : PRINCIPES GÉNÉRAUX**1**

protection du secret de la défense nationale. Elle regroupe l'ensemble des activités visant à protéger et défendre les systèmes numériques¹ et les informations contre d'éventuels incidents de sécurité de nature accidentelle ou intentionnelle et assurer la résilience numérique des entités concernées.

- Cette instruction s'applique :
 - aux états-majors, armées, directions et services relevant de l'autorité du ministre de la défense ;
 - aux établissements publics sous tutelle exclusive du ministère ou relevant de la tutelle de plusieurs ministères, sous réserve d'un accord du/des autre(s) ministères(s) de tutelle ;
 - au Commissariat à l'énergie atomique et aux énergies alternatives (CEA) / Direction des applications militaires (DAM) ;
 - aux entités liées par contrat ou convention au ministère de la défense ou au CEA/DAM ;
 - aux opérateurs d'importance vitale (OIV) relevant des directives nationales de sécurité pour les activités militaires de l'État (DNS AME) et les industries de défense (DNS ID).

1. La protection du secret de la défense nationale et la sécurité numérique

En protégeant la Nation contre l'espionnage des services de renseignement étrangers et les tentatives de déstabilisation par des groupements terroristes, criminels, subversifs ou des individus isolés, la protection du secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation. La sécurité numérique, quant à elle, participe à la protection des informations classifiées au titre du secret de la défense nationale, de même qu'à celles portant la mention *Diffusion Restreinte* ou sensibles.

La divulgation à un tiers non qualifié (personne physique ou morale) d'informations classifiées ainsi que la perturbation ou l'intrusion dans un système numérique peut avoir des conséquences extrêmement préjudiciables, notamment dans les domaines militaire, scientifique et technique ou industriel, comme en termes de confiance des citoyens envers les institutions. Les informations et supports classifiés (ISC) et les systèmes numériques constituent ainsi des cibles privilégiées pour les services étrangers ou pour toute organisation ou individu souhaitant déstabiliser l'État. Ces derniers peuvent agir par la captation frauduleuse d'informations classifiées, *Diffusion Restreinte* ou sensibles, le détournement d'informations ou la diffusion publique de fausses informations, ou porter atteinte à la disponibilité, l'intégrité, la confidentialité et la traçabilité des données de systèmes numériques. Indépendamment du caractère malveillant, voire hostile, de certains actes, la négligence ou la méconnaissance de la

¹ Les systèmes numériques d'une entité incluent l'ensemble organisé des ressources permettant de collecter, traiter, transmettre et stocker les données sous format numérique. Il peut s'agir de systèmes d'information et de communication ou de services numériques.

TITRE 1 : PRINCIPES GÉNÉRAUX**1**

réglementation par le personnel, notamment celui manipulant des informations et supports classifiés font également courir le risque d'une compromission du secret ou d'atteinte à une fonction critique portée par un système numérique.

Ces menaces justifient la mise en place d'un cadre juridique précis régissant la protection du secret de la défense nationale, exposé dans l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (IGI 1300), approuvée par arrêté du Premier ministre.

Les dispositions de l'IGI 1300 sont également applicables à la protection des informations et supports classifiés étrangers confiés à la France en vertu d'un accord général ou spécifique de sécurité, ainsi qu'à ceux de l'OTAN et de l'UE. Elles sont complétées par les dispositions prévues par ces accords, l'instruction interministérielle n° 2100 pour l'OTAN et l'instruction générale interministérielle n° 2102 pour l'UE.

L'instruction interministérielle (II) 901 complète les dispositions fixées par l'IGI 1300 et précise les conditions de sécurité qui entourent la manipulation d'informations *Diffusion Restreinte* et les systèmes numériques portant cette mention de protection.

2. Déclinaison par le ministère de la défense

La politique de protection du secret appliquée par le ministère décline les mesures arrêtées par le Premier ministre, nécessaires à la protection des informations et supports classifiés français ou étrangers confiés à la France tel que défini par l'article L.2311-1 du code de la défense. La présente instruction ministérielle définit les modalités d'application de ces mesures en les adaptant aux spécificités du ministère.

- Elle reprend les récentes évolutions apportées par la réforme de la protection du secret de la défense nationale, notamment :
 - la nouvelle nomenclature de classification (*Secret*, *Très Secret*) ;
 - le renforcement de la sécurité des informations et supports classifiés pendant leur transport et les nouvelles règles techniques relatives à la protection des informations classifiées dématérialisés et des systèmes d'information classifiés.
- Elle rappelle les obligations en matière de protection du secret pour les personnes morales liées par contrat ou convention avec le ministère ou avec le CEA/DAM, en particulier les entreprises de défense liées aux établissements publics sous tutelle du ministère de la défense.
- Elle traduit également les dispositions de l'IGI 1300 favorisant la déclassification des informations et supports lorsque nécessaire, en particulier l'apposition systématique d'une date d'échéance de classification, la révision régulière de la classification des informations et supports classifiés tout au long du cycle de vie et notamment lors des inventaires annuels, la prise en compte des nouvelles dispositions du code du patrimoine.
- Elle tient compte des particularités du ministère et apporte ainsi les précisions nécessaires relatives à la typologie des enquêtes administratives² pour le

² Conformément à l'article L.114-1 du code de la sécurité intérieure.

TITRE 1 : PRINCIPES GÉNÉRAUX**1**

renseignement et la sûreté, à la formation, aux missions et tâches de l'officier de sécurité (OS), de l'officier de sécurité des systèmes d'information (OSSSI) ou aux modalités des contrôles, audits et inspections ainsi qu'à l'application de mesures adaptées aux opérations militaires.

- Elle fixe en annexes des modèles de documents, en complément de ceux définis par l'IGI 1300. Ils constituent les seuls autorisés pour le ministère de la défense et l'ensemble des entités publiques et privées concernées par la présente instruction, à l'exclusion de tout autre.
- Elle prend en compte les évolutions apportées par le décret sur le système d'information de l'État et par l'IGI 1337.
- Elle rappelle surtout que la protection des informations repose sur des règles convergentes pour l'accès direct (physique) au support comme pour l'accès indirect (logique) à l'information. Cette convergence impose la mise en cohérence des deux chaînes de protection du secret et de sécurité numérique. À ce titre, la complémentarité de l'OS et de l'OSSI constitue la pierre angulaire de la sécurité, à intégrer dans les procédures de désignation comme dans les organisations internes.

En complément, la présente instruction fixe également les consignes à respecter pour la protection des informations à caractère sensible. Au sens de cette instruction, une information ou un support sensible est une information ou un support non classifié ou non protégé par la mention *Diffusion Restreinte* mais qui, s'il était révélé à des personnes non autorisées (*via* tout moyen de communication, vers le cercle professionnel ne disposant pas du besoin d'en connaître ou dans le cadre de l'environnement personnel) ou s'il était altéré ou rendu indisponible, pourrait porter atteinte aux objectifs du ministère, des organismes placés sous son autorité, sa tutelle ou liés par contrat ou convention, ou à la protection de leur personnel³.

Ainsi, sont considérées comme sensibles :

- l'ensemble des informations protégées par des mentions spécifiques (*Confidentiel médical, Confidentiel industrie*, par exemple), énumérées dans les fiches 7.3 à 7.5 ;
- les données à caractère personnel comportant la mention de la qualité de militaire (DCPM) telles que précisées dans la fiche 3.11 ;
- plus largement, les informations stratégiques, opérationnelles et organisationnelles, les informations techniques et technico-commerciales, les informations commerciales et les données économiques et financières, les savoir-faire propres au ministère de la défense et à la mise en œuvre ou au maintien en condition de ses matériels.

Pour précision, la mention *Diffusion Restreinte* ou toute autre mention spécifique de protection n'est pas, à elle seule, de nature à restreindre le droit de communication des archives et documents administratifs tel qu'il est fixé par les dispositions respectives

³ La définition proposée ici se distingue, sans la remettre en cause, de celle établie par la loi informatique et libertés (LIL) et le règlement général de protection des données (RGPD). Ces textes définissent les informations sensibles comme des données relatives aux origines raciales ou ethniques des personnes, à leurs opinions politiques, philosophiques ou religieuses, à leur santé ou à leur orientation sexuelle ainsi que les données biométriques, génétiques et relatives à la vie sexuelle des personnes.

TITRE 1 : PRINCIPES GÉNÉRAUX**1**

des codes du patrimoine et des relations entre le public et l'administration⁴. Ces mentions ont pour seul objet d'alerter le détenteur des informations ou supports concernés quant à la nécessaire discrétion dont il convient de faire preuve afin d'éviter d'en révéler l'existence ou de les communiquer à des personnes n'ayant pas le besoin d'en connaître.

De plus, la présente instruction s'applique aux informations et supports classifiés, portant la mention *Diffusion Restreinte* et sensibles mais aussi aux données numériques qui constituent ces informations, selon la définition que l'IGI 1300 précise dans son glossaire introductif. Les données numériques sont ainsi des représentations dans un système numérique de tout ou partie d'une information. Elles sont donc protégées ou classifiées au même niveau que l'information qu'elles décrivent.

Il appartient au responsable d'organisme⁵ émetteur de définir les types d'informations, supports et données qu'il considère comme sensibles et d'orienter ou restreindre autant que nécessaire leur diffusion. Quel que soit le niveau de protection de ces informations et des données qui les constituent, de leurs supports ou des systèmes numériques associés, elles doivent respecter les principes de disponibilité, d'intégrité, de confidentialité et de traçabilité à chaque instant de leur circulation ou de leur détention.

Organisée sous forme de fiches techniques, la présente instruction facilite l'appropriation de la réglementation relative à la protection des informations et des données par les acteurs du ministère. Si la plupart de ces fiches ont une portée générale, certaines sont néanmoins adressées à des publics spécifiques (par exemple, les entités contractantes pour le titre 6 traitant de la sécurité des systèmes numériques⁶).

Les modalités particulières qui s'appliquent aux seules personnes morales liées par contrat ou convention au ministère ou au CEA/DAM sont signalées par un encadré dans le corps du texte.

Pour l'ensemble de l'instruction, chaque dérogation mentionnée est instruite sur la base d'une analyse de risques et fait l'objet d'une décision formalisée.

3. Périmètre d'application de l'IM 900 et mise à jour

La présente instruction est principalement destinée à l'usage des officiers de sécurité et officiers de sécurité des systèmes d'information, maillons essentiels de la chaîne de protection du secret. Elle permet, plus largement, une meilleure sensibilisation aux

⁴ À l'exception des identités des agents des services de renseignement ou de formations spécifiques, protégés par l'article 413-13 du code pénal.

⁵ Au titre de la présente instruction, tout service de l'État (services centraux, services déconcentrés, services à compétence nationale, organismes extérieurs), personnes morales ayant accès, même à titre provisoire, à des informations et supports classifiés ou protégés par la mention de protection *Diffusion Restreinte* ou à des informations sensibles.

⁶ Les entités du département ministériel sont astreintes à l'instruction ministérielle (IM) n° 7326/ARM/CAB du 25 juin 2018, relative à la PSSI du ministère.

TITRE 1 : PRINCIPES GÉNÉRAUX**1**

enjeux de la protection du secret de la défense nationale, comme de toutes les informations et données nécessitant une protection adaptée.

Cette instruction est applicable :

- aux états-majors, armées, directions et services relevant de l'autorité du ministre de la défense ;
- aux établissements publics sous tutelle exclusive du ministère ainsi qu'au CEA/DAM⁷ ; à l'exception du titre 6, qui s'applique uniquement aux personnes morales liées par contrat ou convention au ministère de la défense ou au CEA/DAM ;
- aux établissements sous tutelle de plusieurs ministères, sous réserve d'un accord du/des autre(s) ministère(s) de tutelle ;
- aux personnes morales liées par contrat ou convention au ministère de la défense ou au CEA/DAM, aux opérateurs d'importance vitale (OIV) relevant des directives nationales de sécurité pour les activités militaires de l'État (DNS AME) et les industries de défense (DNS ID).

La présente instruction est applicable dans le respect de l'organisation du contrôle gouvernemental de la dissuasion (CG) défini par les articles R*1411-7 et suivant du code de la défense.

La mise à jour des différentes fiches de la présente instruction, en fonction des évolutions législatives ou réglementaires, voire des pratiques, est effectuée par le moyen d'instructions modificatives signées par délégation du ministre par le haut fonctionnaire correspondant de défense et de sécurité (HFCDS)⁸.

L'ensemble des dispositions de la présente instruction est complété par la politique de protection du secret (PPS), rédigée par chaque officier de sécurité. Le fonctionnaire de sécurité de défense (FSD) est rendu destinataire des PPS rédigées par les officiers de sécurité de niveau 1 du ministère.

⁷ Tout comme les entités du département ministériel, ces établissements sont astreints à l'instruction ministérielle (IM) n° 7326/ARM/CAB du 25 juin 2018, relative à la PSSI du ministère.

⁸ Après avis du SGDSN, le HFCDS fait publier la dernière version complète de l'instruction.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

INTRODUCTION : CHAÎNES FONCTIONNELLES DE LA PROTECTION DU SECRET

Références :

- IGI 1300 – 2.2
- IM n° 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées (PSSI-M)

Points clés

- Le responsable d'un organisme manipulant des informations et supports classifiés assume la responsabilité des mesures de sécurité relatives à la protection du secret de la défense nationale.
- La protection du secret, assurée par le responsable d'organisme, s'appuie sur deux chaînes : la chaîne de protection du secret, dirigée par le fonctionnaire de sécurité de défense (FSD) et la chaîne de sécurité numérique, dirigée par le fonctionnaire de sécurité des systèmes d'information (FSSI). Cette dernière inclut la sécurité des articles contrôlés de la sécurité des systèmes d'informations (ACSSI).
- Afin d'assurer une cohérence d'ensemble de la protection, les acteurs des deux chaînes doivent travailler en collaboration étroite, en particulier pour garantir la protection physique et logique des systèmes d'information.
- Le titulaire d'un contrat endosse également une responsabilité fixée par le plan contractuel de sécurité. Ce dernier énumère les dispositions particulières à l'exécution du contrat pour la protection des informations et supports classifiés ou protégés et aux systèmes d'information soumis à la présente instruction.
- Chaque acteur de la protection du secret, quelle que soit la chaîne à laquelle il appartient, doit pouvoir être remplacé à tout moment afin d'assurer la permanence de la fonction.

1. Le niveau ministériel

Le **ministre** est responsable de la protection du secret de la défense nationale et en contrôle l'application dans son champ d'attribution. Il fixe, au travers de la présente instruction, les exigences à respecter pour les entités placées sous son autorité ou sa tutelle ainsi que pour les autres entités relevant de son champ de compétences.

Il est assisté du **haut fonctionnaire correspondant de défense et de sécurité, chef du cabinet militaire (CM1)**, qui anime et coordonne la politique de défense et de sécurité.

Le HFCDS est assisté par la **direction de la protection des installations, moyens et activités de la défense (DPID)**, dont le directeur est HFCDS adjoint, **qui agit en tant que service du HFCDS (S-HFCDS)**. La DPID anime les chaînes fonctionnelles de la protection du secret. Elle dispose notamment d'un **fonctionnaire de sécurité de défense (FSD)** et d'un **fonctionnaire de sécurité des systèmes d'information (FSSI)** (cf. fiche 2.1).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2. La chaîne fonctionnelle de protection du secret

Elle s'assure de la protection des informations et supports classifiés ainsi que de celle des informations et supports *Diffusion Restreinte* ou sensibles. Elle a pour finalité d'assurer la sécurité relative aux personnes physiques et morales, de garantir la gestion et la protection physique des informations et supports classifiés, protégés par la mention *Diffusion Restreinte* ou sensibles, de s'assurer de la conformité des lieux abritant des éléments couverts par le secret⁹, de procéder aux contrôles et inspections nécessaires et de proposer toutes dispositions destinées à renforcer l'efficacité des mesures de protection mises en place.

Le fonctionnaire de sécurité de défense est chargé d'accompagner les officiers de sécurité de niveau 1 dans l'animation de leur chaîne fonctionnelle de protection du secret.

Dans chaque organisme, **l'officier de sécurité** (cf. fiche 2.5), désigné par **le responsable d'organisme** (chef du service ayant accès à des informations et supports classifiés ou chef d'établissement ou représentant légal de la personne morale liée par contrat ou convention avec le ministère de la défense), constitue un maillon de cette chaîne qui contribue en particulier à la mise en application des règles de sécurité.

Le respect du besoin d'en connaître est un des fondements de la protection du secret. En conséquence, nul ne peut être simultanément officier de sécurité de deux organismes distincts.

Afin de relayer et compléter l'action de l'officier de sécurité au plus près des divers établissements du titulaire du contrat au titre duquel sont traités ou détenus des informations et supports classifiés, le responsable d'organisme peut désigner des **officiers de sécurité d'établissements (OSE)**, dans ces établissements sous le contrôle fonctionnel de l'OS. Ils reçoivent, pour cette mission, les orientations et consignes de l'officier de sécurité.

3. La chaîne fonctionnelle de sécurité numérique (SECNUM)

La chaîne de sécurité des systèmes d'information, prévue par l'IGI 1300 est appelée au ministère de la défense, **chaîne de sécurité numérique (SECNUM)**. Elle est animée par le fonctionnaire de sécurité des systèmes d'information et comprend la sécurité numérique, le déploiement et la traçabilité des articles contrôlés de la sécurité des systèmes d'information (ACSSI). Elle s'appuie sur les personnes exerçant la fonction **d'autorité qualifiée en sécurité des systèmes d'information (AQSSI)**, **d'officier de sécurité des systèmes d'information (OSSI)** et de **responsable de la sécurité des systèmes d'information (RSSI)** (cf. fiche 2.6).

⁹ Un lieu abritant des éléments couverts par le secret de la défense nationale est une pièce dans laquelle sont conservés des informations et supports classifiés, quels qu'en soient le niveau et le volume, répertoriée dans la liste des lieux abritant fixée chaque année par arrêté du Premier ministre conformément à l'article 56-4 du code de procédure pénale.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

Au sein des organismes liés par contrat ou convention avec le ministère, la chaîne de sécurité numérique est conduite par le responsable de l'organisme. Elle s'appuie de la même façon sur des personnes exerçant la fonction d'autorité qualifiée en sécurité des systèmes d'information, d'officier de sécurité des systèmes d'information ou de responsable de la sécurité des systèmes d'information.

Pour le département ministériel, l'organisation de la chaîne de sécurité numérique est décrite dans la politique de sécurité des systèmes d'information (PSSI-M).

La chaîne de sécurité numérique assure notamment l'élaboration, la diffusion et la promotion de la réglementation et des exigences particulières en matière de sécurité des systèmes numériques, y compris ceux contribuant à l'exécution des contrats ou conventions avec le ministère. Elle contrôle leur application. Elle veille au déploiement, à la gestion et à la traçabilité des articles contrôlés de la sécurité des systèmes d'information (ACSSI). Elle est notamment chargée de vérifier l'adéquation des moyens de communication sécurisés avec les besoins de son entité et contribue à la prescription des inspections et contrôles nécessaires. L'ensemble de la chaîne de sécurité numérique est indépendant des chaînes métiers et des chaînes numériques pour lesquelles elles est amenée à conduire ou prescrire des vérifications, contrôles ou inspections.

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI), désignée par le ministre ou le responsable d'un organisme contractant privé ou d'un organisme public autre qu'un établissement public est responsable de la sécurité numérique auprès d'un service ou d'une direction du ministère, ou d'une entité relevant du ministère. Elle travaille en collaboration avec le fonctionnaire de sécurité des systèmes d'information et est chargée d'organiser et d'animer, pour son périmètre de responsabilités¹⁰, la chaîne de sécurité numérique placée sous son autorité. L'autorité qualifiée alloue les ressources nécessaires à la sécurité des systèmes numériques de son périmètre de responsabilité et s'assure que les risques « cyber » ou numériques sont bien gérés. Elle contrôle l'application des exigences de sécurité numérique auxquelles son organisme est soumis.

L'autorité qualifiée en sécurité des systèmes d'information s'assure de l'élaboration, de la mise en œuvre et du maintien, des plans de continuité et de reprise des activités relevant de son domaine de responsabilité face à des incidents de sécurité.

Le rôle d'autorité qualifiée en sécurité des systèmes d'information est assumé par chaque responsable devant le ministre ou le responsable de l'entité concernée.

¹⁰ Cf. Instruction ministérielle n° 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des Armées.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.1****FONCTIONNAIRE DE SÉCURITÉ DE DÉFENSE ET FONCTIONNAIRE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION****Références :**

- IGI 1300 – 2.1.2.2
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Le fonctionnaire de sécurité de défense et le fonctionnaire de sécurité des systèmes d'information sont respectivement les têtes des chaînes fonctionnelles ministérielles protection du secret et sécurité numérique. Ils sont placés auprès du DPID, adjoint du HFCDS.
- Ils assurent notamment l'élaboration, la diffusion et la promotion de la réglementation et des exigences spécifiques à leur chaîne respective et en font contrôler l'application.
- Le fonctionnaire de sécurité de défense et le fonctionnaire de sécurité des systèmes d'information travaillent en relation étroite.

• Le fonctionnaire de sécurité de défense

Le fonctionnaire de sécurité de défense (FSD) est placé auprès du DPID, adjoint du HFCDS. En tant que tête de chaîne de la protection du secret, le fonctionnaire de sécurité de défense, en lien avec le fonctionnaire de sécurité des systèmes d'information :

- rédige la réglementation relative au secret propre au ministère de la défense ;
- définit les modalités de protection du secret de la défense nationale au niveau du ministère de la défense *via* des mesures de protection des informations et supports, des informations sensibles et des documents de niveau *Diffusion Restreinte* ;
- fait contrôler l'application des mesures relatives au secret sur le périmètre du ministère de la défense ;
- pilote la chaîne de protection du secret. À cette fin, il est assisté des officiers de sécurité de niveau 1 ou centraux, réunis en collège des officiers de sécurité que préside le fonctionnaire de sécurité de défense.

Ses responsabilités font l'objet d'une note du DPID.

• Le fonctionnaire de sécurité des systèmes d'information

Le fonctionnaire de sécurité des systèmes d'information (FSSI) est placé auprès du DPID, adjoint du HFCDS. En tant que tête de chaîne de sécurité numérique, le fonctionnaire de sécurité des systèmes d'information en lien avec le fonctionnaire de sécurité de défense :

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.1**

- porte la réglementation interministérielle à la connaissance des différents organismes ;
- élabore la réglementation propre au ministère de la défense ;
- définit les mesures concernant la sécurité des systèmes numériques notamment classifiés, en définissant pour chaque type de système numérique les mesures de protection précisées dans la politique de sécurité des systèmes d'information (PSSI-M) du ministère de la défense ;
- s'assure du contrôle, et peut le cas échéant contrôler directement, l'application de la réglementation et l'efficacité des mesures prescrites ;
- veille à la bonne organisation de la chaîne sécurité numérique en matière de sensibilisation et de formation du personnel ;
- organise la chaîne fonctionnelle des articles contrôlés de la sécurité des systèmes numériques au travers de la directive centrale ministérielle relative aux articles contrôlés de la sécurité des systèmes d'information.

Au sein du ministère, pour l'assister dans l'exécution de ses attributions, le fonctionnaire de sécurité des systèmes d'information s'appuie sur les officiers de sécurité des systèmes d'information (OSSSI) de niveau 1 ou centraux (cf. fiche 2.6), organisés en chaîne. Il travaille en collaboration étroite avec l'autorité qualifiée en sécurité des systèmes d'information ou son représentant (RAQSSI).

Le fonctionnaire de sécurité de défense et le fonctionnaire de sécurité des systèmes d'information diffusent la réglementation vers les personnes morales par l'intermédiaire du service du ministère contractant notamment *via* la DGA.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.2****SERVICES ENQUÊTEURS DU MINISTÈRE DE LA DÉFENSE****Références :**

- Code de la défense – articles L.1332-2-1, L.2362-1, L.4123-9-1
- Code de la sécurité intérieure – articles L.114-1 et R.114-1 à R.114-6
- Code pénal – article R.413-5-1
- IGI 1300 – 2.5.2, 3.2, 3.3.1.3, 4.4.1.4 et 4.4.1.5, 5.3.3.1, 6.1.3

Points clés

- La direction du renseignement et de la sécurité de la défense (DRSD) est le service dont dispose le ministre pour exercer ses responsabilités en matière de protection du personnel, des informations, du matériel et des installations sensibles de son domaine d'attribution.
- Désignée par le Premier ministre comme service enquêteur en matière de protection du secret de la défense nationale pour la sphère de défense, la DRSD mène les enquêtes administratives pour le renseignement et la sûreté (EARS) nécessaires pour détecter toute vulnérabilité dans ce domaine.
- Elle conseille et inspecte les états-majors, directions, services, les organismes sous tutelle du ministère de la défense, les organismes d'importance vitale et les personnes morales sous contrat ou convention avec le ministère de la défense pour vérifier le respect des dispositions réglementaires, les mesures de protection physique des locaux et les règles d'accès aux lieux ainsi que les mesures de protection logique des systèmes d'information.
- La direction générale de la sécurité extérieure (DGSE) est également un service enquêteur, au sens de l'IGI 1300 et agit pour son propre périmètre. Elle vérifie, dans le cadre de la contractualisation réalisée avec des personnes morales de droit privé, le respect des dispositions réglementaires de protection physique des locaux et les règles d'accès aux lieux ainsi que les mesures de protection logique des systèmes d'information.

1. Missions de la DRSD dans le cadre de la protection du secret

- En sa qualité de **service enquêteur** :

Elle réalise des enquêtes administratives pour le renseignement et la sûreté qui visent à s'assurer que le comportement d'une personne n'est pas incompatible avec l'exercice de la fonction ou l'accomplissement de la mission envisagée (cf. fiche 3.9).

Ces enquêtes sont réalisées en particulier :

- préalablement au recrutement des agents du ministère de la défense (civils et militaires) ;

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.2**

- préalablement à l'habilitation des personnes physiques¹¹ et morales devant accéder à des informations et supports classifiés ;
 - préalablement à la délivrance d'autorisations d'accès à une zone¹² ;
 - en cours de carrière, en vue de s'assurer que le comportement d'une personne n'est pas devenu incompatible avec les fonctions ou les missions exercées¹³ (cf. notamment lutte contre la radicalisation) ;
 - sur les personnes accédant à des traitements de données à caractère personnel comportant la mention de la qualité de militaire¹⁴.
- Elle rend également des **avis techniques** sur l'aptitude des locaux et des systèmes d'information à abriter des informations et supports classifiés pour les organismes relevant du périmètre de compétences du ministère.
 - Elle **conseille** les états-majors, directions, services et les différents échelons du commandement, les établissements publics sous tutelle du ministère ainsi que les personnes morales en relation avec la défense (au sens de l'article D.3126-7 du code de la défense), en particulier pour la mise en œuvre des mesures décrites dans la présente instruction.
 - Elle **réalise des inspections** et des contrôles visant à évaluer les mesures de sécurité mises en œuvre dans les domaines de la protection physique et de la sécurité numérique pour assurer la protection des informations sensibles, *Diffusion Restreinte* et classifiées. Ces missions sont réalisées au sein des armées, organismes, établissements, points d'importance vitale et installations prioritaires de défense placés sous l'autorité du ministre, des organismes et emprises qui en relèvent, des établissements publics sous tutelle du ministère ainsi que dans les organismes sous convention ou titulaires de contrats intéressant la défense ou sous-traités à son profit et nécessitant la prise de précautions particulières¹⁵. Ses inspections font l'objet d'un compte-rendu adressé au ministre ainsi qu'aux organismes ayant le besoin d'en connaître.

2. Organisation

En matière de protection du secret, la DRSD est organisée en trois niveaux distincts :

- le niveau local, qui est le contact privilégié de l'officier de sécurité de niveau 3 (cf. fiche 2.5) ;

¹¹ Personnel militaire ou civil relevant du ministère de la défense ou employé dans les organismes et personnes morales liées par contrat ou convention au ministère travaillant à son profit et des personnes morales devant accéder à des informations et supports classifiés ; personnel militaire de la gendarmerie nationale.

¹² À l'exception du CEA/DAM pour lequel le COSSEN est compétent.

¹³ Articles L.114-1 et R.114-6-1 du code de la sécurité intérieure.

¹⁴ Article L.4123-9-1 du code de la défense (périmètre : secteur privé).

¹⁵ Hors installations nucléaires intéressant la dissuasion ne relevant pas du ministre de la défense au sens de l'article R*.1411-9 du code de la défense.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.2**

- le niveau zonal, qui assure une coordination des postes locaux avec une vision géographique plus vaste. Il participe à la mission de contrôle avec, notamment, les visites post-inspections ;
- le niveau central, qui anime la fonction contre-ingérence, en milieu militaire comme dans l'industrie de défense, conduit et réalise les inspections.

3. Missions de la DGSE en tant que service enquêteur

La DGSE conduit les enquêtes administratives propres à son personnel ainsi que celles concernant les personnes morales qui lui sont liées par contrat ou convention et le personnel de ces dernières.

Elle réalise les **inspections et contrôles** en application des instructions et directives relatives à la protection du secret au sein des organismes sous convention ou titulaires de contrats intéressant la défense ou sous-traités à son profit et nécessitant la prise de précautions particulières.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.3****AUTORITÉS D'HABILITATION DU MINISTÈRE DE LA DÉFENSE****Références :**

- Arrêté du 21 mars 2012 modifié¹⁶ portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale
- IGI 1300 – chapitres 3 et 4

Points clés

- L'autorité d'habilitation est l'autorité décisionnaire en la matière. Ce pouvoir du ministre est délégué, par voie réglementaire, à certaines autorités qui lui sont subordonnées.
- L'autorité d'habilitation pour toutes les personnes morales travaillant au profit du ministère de la défense et du CEA/DAM, à l'exception de celles de la DGSE pour son propre périmètre, est la DGA.
- Le SGDSN est l'autorité d'habilitation pour le niveau *Très Secret* faisant l'objet de classifications spéciales et pour les niveaux COSMIC TRES SECRET et TRES SECRET UE sauf délégations éventuellement accordées.

L'autorité d'habilitation est **l'autorité compétente pour émettre la décision d'habilitation ou la décision de refus d'habilitation**, en fonction notamment des conclusions transmises par le service enquêteur.

Le secrétaire général de la défense et de la sécurité nationale (SGDSN) est l'autorité d'habilitation, par délégation du Premier ministre, pour les demandes d'habilitation au niveau *Très Secret* faisant l'objet d'une classification spéciale, ainsi que, sauf délégations éventuellement accordées, aux niveaux *Très Secret COSMIC* et *Très Secret UE*.¹⁷

Par voie réglementaire, le ministre de la défense **délègue son pouvoir d'habilitation** à des autorités qui lui sont subordonnées, avec mention du périmètre des compétences associées, au profit du personnel placé sous leur autorité. Ces délégataires peuvent, si nécessaire, déléguer leur signature à certains subordonnés choisis. Reçoivent, notamment, délégation de pouvoir du ministre les autorités mentionnées ci-dessous.

¹⁶ Notamment par l'arrêté du 28 avril 2017 prenant en compte les transferts de responsabilités pour les habilitations liées au CEA/DAM.

¹⁷ Le *Très Secret UE* et le *Très Secret COSMIC* sont les équivalents UE et OTAN du *Très Secret*.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.3

1. Pour les niveaux **Secret** et **Très Secret** (hors classifications spéciales) :

En administration centrale du ministère de la défense et pour les autorités directement rattachées au ministre :

- haut fonctionnaire correspondant de défense et de sécurité du ministère de la défense ;
- chefs d'état-major ;
- délégué général pour l'armement ;
- secrétaire général pour l'administration ;
- directeurs généraux ;
- directeurs et chefs de service d'administration centrale ;
- chef du Contrôle Général des Armées et membres des corps d'inspection directement rattachés au ministre ;
- délégué à la sûreté nucléaire et à la radioprotection pour les activités et installations intéressant la défense.

Hors administration centrale : les commandants organiques et opérationnels des forces et commandants interarmées.

Le personnel militaire de la gendarmerie nationale, d'active ou de réserve, placé pour emploi au sein du ministère de la défense dans les formations des gendarmeries spécialisées est habilité par une autorité désignée par un arrêté portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale (cf. arrêté en référence).

2. Pour le niveau **Secret** :

- les commandants des formations administratives ou des organismes administrés comme tels ;
- les commandants des écoles de formation ;
- les directeurs ou chefs des organismes n'appartenant pas à l'administration centrale du ministère de la défense.

Le **délégué général pour l'armement** et le **directeur général de la sécurité extérieure**, **seulement pour leur périmètre de compétences**, ont délégation de pouvoir du ministre pour signer les **décisions d'habilitation des personnes morales** candidates ou titulaires d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés ainsi que des personnes physiques qui en dépendent.

Afin de remplir cette mission au nom du ministre, la DGA dispose d'une entité spécifique, le **service de la sécurité de défense et des systèmes d'information (SSDI)**. Ce service est aussi chargé de prononcer les décisions d'agrément des officiers de sécurité, proposés par les entités habilitées, après avis du service enquêteur (officier de sécurité, officier de sécurité des systèmes d'information et leurs adjoints), hors périmètre DGSE.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.4****RESPONSABILITÉS DU RESPONSABLE D'ORGANISME****Références :**

- IGI 1300 – 2.2.1
- Instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics

Points clés

- Le responsable d'organisme exerce l'entière responsabilité de la protection du secret dans son organisme (cf. glossaire IGI 1300).
- Le responsable d'organisme (commandant de formation administrative ou chef d'établissement - CFA/ CE - ou représentant légal de la personne morale) est le responsable local de la sécurité de son personnel, de ses matériels et de ses installations. Ce champ de responsabilités englobe la protection du secret (informations et supports classifiés, articles contrôlés de la sécurité des systèmes d'information, lieux abritant des informations et supports classifiés, habilitations du personnel), celle des informations et supports protégés par la mention *Diffusion Restreinte* et des informations sensibles ainsi que la sécurité des systèmes numériques.
- Il désigne un officier de sécurité (OS) et un officier de sécurité des systèmes d'information (OSSI) pour l'appuyer dans l'exercice de ses responsabilités. Ils animent respectivement la chaîne de protection du secret et celle de la sécurité numérique, sous l'autorité du responsable d'organisme.

Le responsable d'organisme est le responsable de l'ensemble des locaux et de la sécurité de son personnel, de ses matériels et de ses installations. Dans ce cadre, il valide la politique de protection du secret rédigée par son officier de sécurité, assume la responsabilité des mesures de sécurité relatives à la protection du secret (documents imprimés ou dématérialisés, réseaux, matériels classifiés, habilitation du personnel), à la protection des installations (notamment les lieux abritant des informations et supports classifiés) et à la sécurité des systèmes numériques.

Il organise les deux chaînes fonctionnelles de protection du secret et de sécurité numérique. A cet effet, il désigne, après réception de la décision d'agrément, un officier de sécurité, un officier de sécurité des systèmes d'information et, dans la mesure du possible, un adjoint pour chacun d'eux, au sein de son organisme (cf. fiche 2.5 et 2.6). À défaut d'officier de sécurité et d'officier de sécurité des systèmes d'information, le responsable d'organisme se charge lui-même de l'accomplissement des tâches relatives à la protection du secret pour son entité.

Dans certains cas exceptionnels, notamment du fait de la petite taille de l'organisme, le responsable d'organisme peut également occuper la fonction d'officier de sécurité ou d'officier de sécurité des systèmes d'information.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE
2.4

Missions	Tâches à réaliser
Garantir la protection du secret et la sécurité numérique au sein de son entité.	Contrôle de l'application de la politique de protection du secret (IGI 1300, IGI 1337, présente instruction, PSSI-M, dispositions contractuelles applicables pour les personnes morales, etc.).
Organiser la chaîne de protection du secret et la chaîne de sécurité numérique.	<p>Désignation (nominative) de l'officier de sécurité, l'officier de sécurité des systèmes d'information de leurs adjoints ou suppléants.</p> <p>Création d'un bureau de protection du secret, obligatoire pour le <i>Très Secret</i>.</p> <p>Validation de la politique de protection du secret au sein de son organisme, rédigée par son officier de sécurité.</p> <p>Pour les organismes privés et les établissements publics : désignation d'une autorité qualifiée pour la sécurité des systèmes d'information</p> <p>Pour les organismes publics autres que les établissements publics de l'Etat : identification de son autorité qualifiée.</p>
Veiller à la bonne gestion des habilitations et à la mise à jour annuelle, ou lors de réorganisation de service, du catalogue des emplois.	Par délégation de pouvoir du ministère de la défense, pour le département ministériel : habilitations pour le niveau <i>Secret</i> .
Assurer la formation du personnel.	Veille à l'organisation de l'instruction de sécurité et de la sensibilisation du personnel placé sous ses ordres en matière de protection du secret et de sécurité numérique.
Organiser le système général de sécurité en fonction du degré de sensibilité de ses installations.	Demander les créations de zones protégées, créer les zones réservées et rédiger un plan de protection du site définissant les règles d'accès et de circulation.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.5****OFFICIER DE SÉCURITÉ****Référence :**

- IGI 1300 – 2.2.2.1

Points clés

- L'officier de sécurité (OS) est un maillon essentiel de la chaîne de protection du secret, des informations et supports protégés par la mention *Diffusion Restreinte* et des informations sensibles. Il rédige la politique de protection du secret de son organisme et veille à son application. Il forme le personnel de la chaîne de protection du secret qui lui est subordonné et sensibilise régulièrement l'ensemble du personnel habilité. Il dirige généralement le bureau de protection du secret (BPS). Il travaille en liaison étroite avec l'officier de sécurité des systèmes d'information (OSSI).
- L'officier de sécurité dispose d'un niveau hiérarchique suffisant et des moyens nécessaires pour accomplir ses missions. Sa prise de fonction est conditionnée par l'obtention d'une décision d'habilitation au niveau requis et d'un agrément du service enquêteur ou de la DGA.
- Au-delà du seul domaine de la protection du secret, le ministère de la défense recommande que les officiers de sécurité de son périmètre soient aussi chargés de tout ou partie des autres domaines de la défense-sécurité, notamment de la protection physique des installations.

L'officier de sécurité (OS) exerce de larges prérogatives dans le domaine de la défense-sécurité (protection des installations, du personnel et des biens pour les organismes étatiques, etc.) afin de s'assurer de la cohérence de l'ensemble des dispositions. La présente fiche se borne à détailler ses seules attributions en matière de protection du secret, de protection des informations et supports protégés par la mention *Diffusion Restreinte* et celle des informations sensibles.

1. Attributions en matière de protection du secret

L'officier de sécurité met en œuvre et peut diriger les moyens de protection du secret (bureau de protection du secret, structure de sécurité). Il rédige à cet effet la politique de protection du secret de son organisme. Il assure la formation du personnel de la chaîne fonctionnelle de protection du secret et la sensibilisation du personnel, détenteur d'informations et supports classifiés ou non, de son entité. Il coordonne son action, le cas échéant, avec l'officier de sécurité des systèmes d'information (OSSI).

Un **officier de sécurité adjoint (OSA)** peut être nommé auprès de l'officier de sécurité par le responsable d'organisme, dans les mêmes conditions que celles fixées aux paragraphes 2 et 3 de la fiche 2.5. Cet officier de sécurité adjoint dispose des mêmes compétences que l'officier de sécurité en titre. Il assure également sa suppléance en son absence. Ses prérogatives et responsabilités sont fixées par le responsable d'organisme.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.5**

L'officier de sécurité est également chargé de la rédaction de la politique de protection du secret, validée ensuite par le responsable d'organisme.

L'officier de sécurité est le contact privilégié, pour son organisme, de l'autorité d'habilitation, du fonctionnaire de sécurité de défense (pour les officiers de sécurité têtes de chaîne) et du service enquêteur.

Lorsqu'un changement apparaît chez la personne morale ou physique habilitée, il en rend compte à sa hiérarchie et à l'autorité d'habilitation et signale au service enquêteur les vulnérabilités des personnes morales ou physiques dont il a connaissance.

En cas de suspicion de compromission, l'officier de sécurité, avec l'officier de sécurité des systèmes d'information le cas échéant, rend compte à sa chaîne hiérarchique, à la chaîne fonctionnelle de protection du secret et en informe le service enquêteur.

Les tâches de l'officier de sécurité en matière de protection du secret sont regroupées en trois principaux domaines d'action : la protection du personnel, celle des informations et supports classifiés, protégés par la mention *Diffusion Restreinte* ou sensibles et celle des lieux abritant des informations et supports classifiés.

Les officiers de sécurité des personnes morales contractantes avec le ministère de la défense sont de surcroît chargés du suivi des exigences de sécurité figurant dans les contrats et les plans contractuels de sécurité.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE
2.5

Les attributions de l'officier de sécurité	
Protection du personnel	Protection des informations et supports classifiés et informations sensibles
<ul style="list-style-type: none"> • Gérer les habilitations et enquêtes administratives (demandes via SOPHIA ou par les gendarmeries spécialisées (GS)). • Tenir à jour le ou les catalogues des emplois (un par réseau et par niveau d'habilitation). • Apprécier les avis de sécurité consécutifs aux enquêtes administratives et établissement des droits d'accès (visiteurs, prestataires, etc.) lorsque l'autorité dont il dépend est le commandant de formation administrative ou chef d'établissement de l'installation. • Suivre et contrôler les autorisations d'accès. • Suivre et contrôler les ressortissants étrangers. • Suivre les séjours à l'étranger (stage, mission, permissions). • Analyser les vulnérabilités du personnel du ou des sites de l'organisme dans lequel il est en fonction, incluant les faits constatés (préjudice moral, discipline, comportement à risque, etc). • Rédiger des compte-rendu de suspicion de compromission transmis au service enquêteur concerné. • Organiser des séances d'instruction ou de sensibilisation garantissant une sensibilisation à une fréquence régulière de chaque agent. • Sensibiliser les agents avant une mission ou un départ à l'étranger. 	<ul style="list-style-type: none"> • Rédiger la politique de protection du secret de son organisme ou du réseau qu'il anime. Elle est adressée à l'ensemble des officiers de sécurité de niveau N-1. Pour les officiers de sécurité de niveau 1, l'adresser également au fonctionnaire de sécurité de défense. • Si désigné par le responsable d'organisme pour cette mission, occuper le poste de responsable du bureau de protection du secret (BPS). • Surveiller, protéger et contrôler les informations et supports classifiés, protégés ou sensibles. • Contrôler le personnel ayant accès aux informations et supports classifiés. • Participer, le cas échéant, au suivi de la sécurité des systèmes numériques classifiés avec l'officier de sécurité des systèmes d'information. • Contrôler l'application des règles de protection, de manipulation et de destruction des informations et supports classifiés¹⁸.
	Protection des lieux abritant des informations et supports classifiés
	<ul style="list-style-type: none"> • Suivre les arrêtés concernant les zones protégées. • Tenir à jour les documents constitutifs des zones réservées (ZR). • Suivre les avis d'aptitude des lieux abritant des informations et supports classifiés. • Suivre les dossiers de consignes, les autorisations d'accès, les visites. • Mettre à jour la liste des lieux abritant relevant de son organisme.

¹⁸ Cf. [annexe 21](#) pour un rappel des principaux documents concernés.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.5

Suivi des contrats et plans contractuels de sécurité de son périmètre

- Tenir à jour la liste des contrats impliquant l'accès ou la détention d'informations et supports classifiés.
- Valider le plan contractuel de sécurité (en lien avec l'OSSI pour les aspects de sécurité numérique).
- Conseiller en matière de prise en compte de la sécurité de défense dans les contrats auprès des acheteurs de son organisme.
- Contrôler le respect des dispositions nécessaires à la protection du secret chez les contractants et éventuels sous-contractants.

2. Désignation

L'officier de sécurité est désigné nominativement par le responsable de l'organisme parmi son personnel¹⁹, s'il satisfait aux conditions suivantes :

- il appartient de façon suffisamment stable à l'organisme : il a une fiche de poste ou a signé un contrat de travail prévoyant cette fonction. La sous-traitance de cette fonction est interdite ;
- il est habilité au niveau requis par la fonction ;
- il reçoit l'agrément du service enquêteur²⁰ ;
- il a validé un stage initial de formation (à défaut, le valide dans l'année suivant sa nomination) ;
- il est de nationalité française si l'organisme est appelé à traiter des informations et supports classifiés portant la mention de protection *Spécial France* ;
- il dispose d'un accès direct au responsable d'organisme et d'un niveau hiérarchique suffisant pour le conseiller ;
- il dispose de tous les moyens nécessaires à l'accomplissement de sa mission.

Ses coordonnées sont détenues par les officiers de sécurité de niveau supérieur.

Pour les organismes désignés opérateurs d'importance vitale (OIV)²¹, le délégué pour la défense et la sécurité (DDS), prévu par la réglementation relative à la sécurité des activités d'importance vitale, peut exercer la fonction d'officier de sécurité. À défaut, cette fonction est exercée par son adjoint ou un subordonné direct. De même, les délégués locaux à la défense et à la sécurité (DDSL) peuvent exercer la fonction d'OS 2 ou 3 ou d'officier de sécurité d'établissement (OSE). Dans tous les cas, un dialogue étroit entre les chaînes d'officier de sécurité et celle des DDS et des DDSL est à rechercher.

¹⁹ Pour les formations militaires, l'officier de sécurité peut être choisi parmi les agents civils ou le personnel militaire d'active ou de réserve opérationnelle. Dans ce dernier cas, le commandant de formation doit s'assurer de la disponibilité opérationnelle du réserviste pour accomplir cette fonction.

²⁰ À l'exception des officiers de sécurité relevant des personnes morales liées par un contrat ou une convention avec le ministère, agréés par la DGA.

²¹ À l'exception du CEA/DAM.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

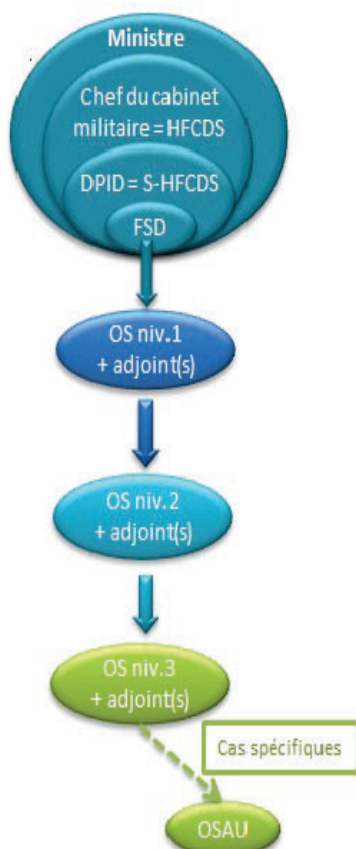
2.5

3. Formation

La formation de l'officier de sécurité relève de la responsabilité du responsable d'organisme qui l'a désigné.

Avant sa prise de fonction (ou dans l'année de sa désignation), l'officier de sécurité suit un stage de formation initiale qualifiant :

- chaque chaîne de sécurité est responsable de la formation des officiers de sécurité, décrite dans la PPS²² ;
- la DPID rédige une directive de formation définissant le socle de compétences des officiers de sécurité pour le périmètre ministériel. Le fonctionnaire de sécurité de défense s'assure de sa bonne application ;
- une actualisation régulière des compétences des officiers de sécurité est recommandée.



Pour les officiers de sécurité des personnes morales liées par contrat ou convention avec le ministère, la formation doit être évaluée régulièrement et acceptée par l'autorité d'habilitation de ces dernières.

4. L'officier de sécurité du département ministériel

Pour chaque autorité directement subordonnée au ministre, la chaîne fonctionnelle de protection du secret permet un maillage territorial et fonctionnel garantissant la couverture de l'ensemble de son périmètre et appliquant le principe de subsidiarité :

- un **officier de sécurité de niveau 1** (OS 1) est placé auprès de chaque autorité immédiatement subordonnée au ministre de la défense. Tête de chaîne et correspondant privilégié du fonctionnaire de sécurité de défense, il est le conseiller de sa hiérarchie, à laquelle il propose l'organisation de la chaîne de protection du secret adaptée aux spécificités de son armée, de sa direction ou de son service. Il est généralement chef du bureau principal de protection du secret de sa chaîne (BPPS – cf. fiche 2.7). Les officiers de sécurité de niveau 1 ne peuvent avoir d'autres fonctions que celles relevant du domaine de la défense-sécurité ;

²² Pour les établissements sous tutelle du ministère, le responsable d'organisme est en charge de la mise en formation de son officier de sécurité, parmi l'offre de stages délivrant les compétences identifiées dans la directive de formation de la DPID.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.5**

- au niveau intermédiaire, il est créé autant de postes **d'officier de sécurité de niveau 2** (OS 2) que nécessaire. Ce dernier est subordonné fonctionnellement à son officier de sécurité de niveau 1, dont il prolonge l'action. Il conseille son DDS régional, s'il existe, ainsi que l'autorité hiérarchique zonale ou fonctionnelle auprès de laquelle il est placé. Il est généralement chef d'un bureau secondaire de protection du secret (BSPS) ;
- chaque formation administrative ou établissement dispose d'un **officier de sécurité de niveau 3** (OS 3), conseiller du commandant de formation administrative ou chef d'établissement et, le plus souvent, chef d'un bureau de protection du secret dont les responsabilités sont précisées dans une note.
- Afin d'assister l'officier de sécurité au sein de l'entité, le commandant de formation administrative ou chef d'établissement peut lui désigner des adjoints :
 - o En cas de traitement d'informations et supports classifiés sur site, d'éloignement important de la portion centrale ou de sensibilité particulière d'une installation, le commandant de formation administrative ou chef d'établissement peut désigner un officier de sécurité adjoint d'unité (OSAU). En sa qualité d'officier de sécurité, l'officier de sécurité adjoint d'unité satisfait aux exigences fixées au paragraphe 2 de la fiche 2.5. Ses responsabilités particulières sont décrites par le commandant de formation administrative ou chef d'établissement.
 - o En l'absence de traitement d'informations et supports classifiés sur site, le commandant de formation administrative ou chef d'établissement désigne un correspondant de sécurité (CS) dont les missions sont fixées par l'OS²³, en lien avec le responsable d'organisme ou le chef de la personne morale de droit privé.

5. L'officier de sécurité au sein d'une personne morale liée par contrat ou convention avec le ministère

L'officier de sécurité est désigné nominativement (cf. IGI 1300 – annexe 19) par le responsable de l'organisme employeur s'il satisfait aux conditions évoquées dans le paragraphe 2 de cette fiche ainsi qu'aux conditions spécifiques suivantes :

- il est habilité au même niveau que la personne morale dont il dépend ;
- il reçoit l'agrément de l'autorité d'habilitation après avis émis par le service enquêteur.

Si plusieurs établissements de l'organisme détiennent des informations et supports classifiés, un **officier de sécurité d'établissement** est désigné dans chacun d'entre eux. Celui-ci doit être employé dans l'établissement (identifié par un numéro de SIRET) pour lequel il est proposé, sauf dérogation prise, après avis du service enquêteur, par

²³ Le correspondant de sécurité ne disposant pas d'un agrément du service enquêteur, il ne peut être en charge de la protection du personnel. A cet effet, il ne peut réaliser les mises en éveil et les mises en garde.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.5

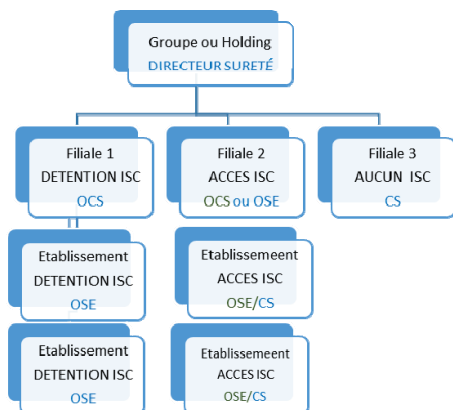
l'autorité d'habilitation de la personne morale. L'officier de sécurité du siège social est alors identifié comme **officier central de sécurité (OCS)** de la personne morale.

Dans le cas des groupes de sociétés ou des sociétés holding, si au moins une société du groupe ou une filiale a accès au secret de la défense nationale, un officier de sécurité de groupe ou de holding peut être désigné pour assurer une cohérence entre la gouvernance et les enjeux de protection du secret.

Le responsable d'organisme peut, en outre, en dehors des établissements détenant ou traitant des informations ou supports classifiés, désigner des **correspondants de sécurité (CS)** placés sous le contrôle opérationnel de l'officier de sécurité ou de l'officier central de sécurité au sein de chaque subdivision physique ou opérationnelle de la personne morale. Ces correspondants de sécurité rendent compte autant que besoin et participent à la sensibilisation du personnel.

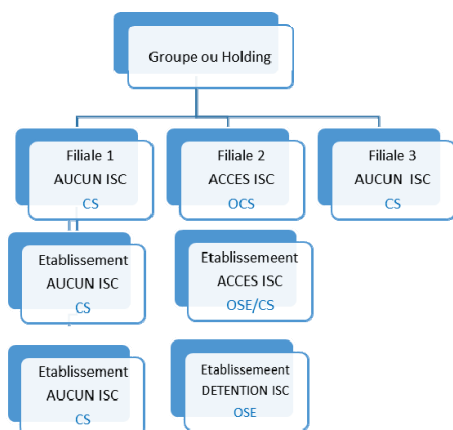
Cas 1 : plusieurs filiales détiennent ou accèdent à des informations et supports classifiés.

En complément, un officier de sécurité de groupe ou de holding peut être désigné. Cette mesure est obligatoire en cas de détention d'informations et supports classifiés et si la personne morale est habilitée. Son rôle vise essentiellement à mettre en cohérence la politique de protection du secret dans l'ensemble du groupe ou de la holding.



TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.5**

Cas 2 : une seule filiale détient ou accède à des informations et supports classifiés.



Processus d'agrément des officiers de sécurité lorsque la DGA est autorité d'habilitation : le service enquêteur transmet un avis d'agrément à la DGA qui décide ou non d'agréer l'officier de sécurité (ce dernier ne peut exercer ses fonctions tant que la DGA ne délivre pas sa décision d'agrément). En cas de refus d'agrément, le représentant de la personne morale propose une autre personne et recommence le processus.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.6****OFFICIER DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DES PERSONNES MORALES LIÉES PAR CONTRAT OU CONVENTION AVEC LE MINISTÈRE DE LA DÉFENSE****Référence :**

- IGI 1300 – 2.2.3.2

Points clés

- L'officier de sécurité des systèmes d'information (OSSI) assure :
 - l'organisation générale de la chaîne de sécurité numérique de l'organisme ;
 - la rédaction de la politique de sécurité numérique de son organisme et en contrôle l'application ;
 - l'organisation de l'homologation²⁴ des systèmes d'information ;
 - le pilotage de la sensibilisation des utilisateurs et des administrateurs des systèmes numériques ainsi que des acteurs de la sécurité numérique de l'organisme.
- Les officiers centraux de sécurité des systèmes d'information des personnes morales sont les correspondants du fonctionnaire de sécurité des systèmes d'information.
- L'officier de sécurité des systèmes d'information coordonne son action avec l'officier de sécurité.
- L'officier de sécurité des systèmes d'information dispose d'un niveau hiérarchique suffisant et des moyens nécessaires pour accomplir ses missions. Sa prise de fonction est conditionnée par l'obtention d'une décision d'habilitation au niveau requis et d'un agrément du service enquêteur ou de la DGA.

Les dispositions suivantes s'appliquent uniquement aux entités liées par contrat ou convention au ministère. Pour les organismes relevant du ministère de la défense et pour les organismes publics sous sa tutelle, les éléments figurent dans l'IM n° 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées.

1. Principes généraux

Employé en sécurité numérique auprès d'une autorité pour l'aider à mettre en œuvre les processus opérationnels et supports qui lui incombent, l'officier de sécurité des systèmes d'information conçoit et met en œuvre un système de management du

²⁴ La démarche d'homologation de sécurité est une obligation préalable à la mise en service du système numérique et repose sur une analyse de risques. Elle permet d'identifier et évaluer ces derniers, d'atteindre puis de maintenir « un niveau de risques acceptable » pour le système numérique considéré au regard du niveau de protection requis.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.6**

système d'information (SMSI), sauf dérogation de l'organisme inspecteur en accord avec l'autorité contractante, notamment dans le cas de petites structures. Il coordonne les moyens liés à sa mission, vérifie la mise en œuvre de la politique de sécurité numérique, des obligations de protection des informations et supports classifiés conseille son autorité et pilote la sensibilisation du personnel concerné. Il coordonne son action avec celle de l'officier de sécurité pour tout ce qui concerne la protection des systèmes d'information de l'organisme et, particulièrement, les systèmes d'information classifiés. Il est désigné dans les mêmes conditions que l'officier de sécurité, est formé (sécurité numérique, articles contrôlés de la sécurité des systèmes d'information, le cas échéant) et dispose de moyens nécessaires pour accomplir ses missions.

L'officier de sécurité des systèmes d'information est en relation régulière avec la DGA/SSDI et son point de contact au sein du service enquêteur.

Dès lors que l'organisme est constitué de plusieurs établissements, le responsable d'organisme désigne un officier central de sécurité des systèmes d'information (OCSSI). Par défaut, l'officier de sécurité des systèmes d'information du siège social est officier central de sécurité des systèmes d'information lorsque l'organisme dispose d'autres établissements, eux-mêmes disposant alors d'**OSSI locaux (OSSI-L)**, placés auprès du responsable de chaque établissement.

Dans certains cas exceptionnels, notamment du fait de la petite taille de l'organisme, le responsable d'organisme peut également occuper la fonction d'officier de sécurité des systèmes d'information.

En fonction de la taille de l'organisme, du niveau de classification des informations traitées et de la nature des systèmes à protéger, l'officier de sécurité des systèmes d'information peut disposer de **correspondants de sécurité des systèmes d'information (CSSI)**, désignés par le responsable d'organisme. Les responsables de la sécurité des systèmes numériques sont désignés par les autorités d'emploi ou le responsable d'organisme. Dans l'accomplissement de leur fonction, ils se coordonnent avec l'officier de sécurité des systèmes d'information pour le développement et l'exploitation des systèmes d'information concernés.

Le **responsable de sécurité des systèmes d'information (RSSI)** pilote la démarche d'intégration de la sécurité du système numérique durant la phase du projet, jusqu'à l'homologation initiale incluse, qu'il est chargé d'instruire sous la responsabilité de l'autorité d'homologation. Après l'homologation initiale et dès que le système est opérationnel, il assure le suivi de la sécurité du système numérique en service jusqu'à sa fin de vie. Il est notamment chargé d'instruire les renouvellements d'homologation. Pour le système dont il a la charge et dans le domaine de la sécurité numérique, il conseille, recommande et propose à l'autorité responsable de l'exploitation du système numérique des règles spécifiques. Il est garant de la cohérence des mécanismes et des procédures de sécurité ainsi que du maintien du niveau de sécurité dans le temps, et de la bonne prise en compte des enjeux de protection des données jusqu'à la fin de vie des systèmes d'information. Il assure principalement les fonctions opérationnelles liées à la sécurité des systèmes numériques soumis à la présente instruction relevant de son périmètre de responsabilité.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.6

Les officiers de sécurité des systèmes d'information disposent, pour faire exécuter tout ou partie des tâches leur incombant en matière de sécurité numérique, de **bureaux de sécurité des systèmes d'information** (BSSI centraux ou locaux) lorsque la taille de l'organisme le permet.

L'officier de sécurité des systèmes d'information doit être indépendant des chaînes numérique ou métier qu'il est amené à contrôler pour garantir la qualité de la remontée d'informations vers le responsable d'organisme qui le nomme.

2. Attributions

Les attributions de l'officier de sécurité des systèmes d'information se répartissent en quatre champs de compétences :

Les attributions de l'officier de sécurité des systèmes d'information	
Politique de sécurité numérique	Suivi des informations et supports classifiés numériques
<ul style="list-style-type: none"> - Valider les procédures d'exploitation de sécurité des systèmes numériques établies par le responsable de la sécurité des systèmes d'information. - S'assurer que les personnes, employées à titre permanent ou occasionnel, administratrices ou utilisatrices d'un traitement numérique comportant des informations classifiées sont habilitées au niveau adéquat. - Faire surveiller en permanence les activités des utilisateurs extérieurs appelés à effectuer des travaux temporaires sur le système numérique et les opérations de maintenance. - S'assurer que les sociétés prestataires de service ont fait l'objet de contrats impliquant l'accès ou la détention d'informations et support classifiés ou de contrats sensibles. - Participer à la rédaction de la politique de protection de secret pour la partie relative aux systèmes numériques, en lien avec l'officier de sécurité. - S'assurer que les exigences de sécurité numérique associées à un contrat avec l'État sont correctement transposées dans les contrats subséquents passés pour la réalisation de ce premier contrat. 	Homologation des systèmes d'information
	<ul style="list-style-type: none"> - En liaison avec l'officier de sécurité, établir des mesures de protection, des consignes particulières relatives à la conservation, la prise en compte et la destruction des supports d'informations classifiées numériques et contrôler leur application²⁵. - Faire tenir à jour le dossier de sécurité des différents systèmes d'information. - Définir l'organisation générale du processus d'homologation, en lien avec le service enquêteur pour l'aptitude informatique des systèmes d'information, y compris des systèmes d'information de sûreté (CADIVS : contrôle d'accès, détection d'intrusion et vidéo-surveillance).

²⁵ Cf. [annexe 21](#) pour un rappel des principaux documents concernés.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.6

Politique de sécurité numérique	Suivi des articles contrôlés de la sécurité des systèmes d'information
<ul style="list-style-type: none"> - S'assurer de l'application, par le personnel d'exploitation et les utilisateurs, des règles de sécurité prescrites. - Piloter la sensibilisation du personnel (utilisateurs et administrateurs en particulier) en matière de sécurité numérique et en lien avec l'OS. - S'assurer que la chaîne de sécurité numérique dispose du niveau de formation requis pour mener efficacement les tâches qui lui incombent. - Vérifier périodiquement le bon fonctionnement des dispositifs de sécurité. - Veiller au respect des procédures opérationnelles de sécurité propres au système de traitement utilisé. - S'assurer de l'aptitude physique des locaux en liaison avec l'officier de sécurité et le poste renseignement sécurité défense (RSD) compétent pour les systèmes d'information classifiés. - Rendre compte de toute suspicion de compromission et incident constaté (chaîne hiérarchique, chaîne de sécurité numérique, officier de sécurité, service enquêteur, autorité contractante, autorité d'habilitation). - Valider, en lien avec l'officier de sécurité, les aspects liés à la sécurité numérique dans les plans contractuels de sécurité. 	<ul style="list-style-type: none"> - Assurer ou s'assurer de la gestion des articles contrôlés de la sécurité des systèmes d'information, qu'ils soient classifiés ou non, du respect des règles de sécurité lors de leur déploiement, du suivi et de leur traçabilité, de leur contrôle et du traitement des incidents de sécurité associés.

En matière de sécurité numérique, l'officier de sécurité des systèmes d'information intervient à tous les stades d'étude, de réalisation, d'utilisation, d'évolution, de démantèlement d'un système numérique et de destruction des supports. Pour ce qui concerne notamment les supports numériques (clés USB, disques durs, moyens ou supports articles contrôlés de la sécurité des systèmes d'information, etc.), l'officier de sécurité des systèmes d'information se coordonne avec l'officier de sécurité.

L'ensemble des attributions de l'officier de sécurité des systèmes d'information fait l'objet d'un ou de documents écrits établissant clairement la nature de la délégation de responsabilité et des pouvoirs sur les moyens associés entre le représentant légal de la personne morale et l'officier de sécurité des systèmes d'information. Par ailleurs, l'officier de sécurité des systèmes d'information coordonne son action avec l'officier de sécurité dans l'élaboration et la validation des contrats et plans contractuels de sécurité sur la dimension sécurité numérique.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.7****BUREAU DE PROTECTION DU SECRET****Références :**

- IGI 1300 – 7.2.1.1, 7.2.1.2, 7.2.2.1 et 7.2.2.2

Point clé

La création d'un bureau de protection du secret (BPS) est obligatoire lorsque l'entité détient des informations et supports classifiés de niveau *Très Secret* ; elle est recommandée pour le *Secret*.

Le bureau de protection du secret (BPS) est la dénomination de la structure constituée dans l'organisme pour s'occuper de la gestion du secret. Par extension, le terme désigne aussi ses locaux. Le bureau de protection du secret est placé sous la responsabilité de l'officier de sécurité.

L'existence d'un bureau de protection du secret est obligatoire pour organiser l'élaboration, le marquage, l'enregistrement, le stockage, l'acheminement, le suivi et la destruction des informations et supports classifiés de niveau *Très Secret*, hors classifications spéciales²⁶. À cette fin, le bureau de protection du secret dispose d'une zone réservée, dans laquelle les tâches afférentes à la gestion du *Très Secret* sont réalisées.

La création de ce bureau est recommandée pour la gestion des informations et supports classifiés de niveau *Secret*. Dans ce cas, la zone réservée n'est pas nécessaire. Le bureau de protection du secret, par ses missions, est différent d'un bureau courrier.

Le bureau de protection du secret assure également la gestion des informations et supports classifiés étrangers. Les informations et supports classifiés UE ou OTAN sont gérés²⁷ par des bureaux d'ordre, dont les modalités de création et les missions sont définies par les textes de référence²⁸. Les missions de ces bureaux d'ordre peuvent être confiées aux bureaux de protection du secret.

Pour la gestion des informations et supports classifiés de niveau *Secret*, en l'absence de bureau de protection du secret ou d'un secrétariat, une ou plusieurs personnes du bureau courrier sont désignées et formées pour assurer le suivi spécifique des informations et supports classifiés.

²⁶ Les informations et supports classifiés de niveau *Très Secret* faisant l'objet d'une classification spéciale répondent à des mesures de protection spécifiques.

²⁷ Élaboration, traitement, stockage, destruction ou acheminement des informations et supports classifiés.

²⁸ II 2100 et IGI 2102.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.7****1. Missions**

Le bureau de protection du secret :

- trace les informations et supports classifiés émis/reçus par son organisme, notamment au travers d'un suivi rigoureux des bordereaux ABB' (cf. fiche 7.8) ;
- contrôle la position des informations et supports classifiés de niveau *Très Secret* via une fiche de suivi, établie pour chaque support et émargée par chaque personne qualifiée en ayant accès, qu'il conserve et rattache au support dès que les nécessités du service permettent de le réintégrer ;
- s'assure de l'établissement d'un inventaire annuel des informations et supports classifiés de niveaux *Secret* et *Très Secret* détenus par son entité, sauf en l'absence de bureau de protection du secret lorsque seuls des informations ou supports classifiés de niveau *Secret* sont gérés par un organisme ;
- participe à la gestion des dossiers d'habilitation du personnel de son périmètre ;
- participe à l'animation des séances d'instruction et de sensibilisation ;
- coordonne l'action du personnel des bureaux de protection du secret qui lui sont subordonnés ;
- participe à la mise à jour du catalogue des emplois de niveau *Très Secret* ou *Secret* ;
- peut organiser le contrôle d'une zone réservée en dehors des heures d'utilisation (fermeture, fonctionnement des systèmes de détection, vidage des corbeilles à papier, absence d'informations et supports classifiés hors meubles de sécurité), sous l'autorité de l'officier de sécurité.

Placées sous la direction de l'officier de sécurité de l'organisme, les activités du bureau de protection du secret sont organisées de telle sorte que les informations traitées, les documents, matériels ou équipements électroniques, reçus, émis et conservés, ne soient accessibles qu'aux personnes qualifiées.

Le personnel qui y est affecté est employé directement par l'organisme et est habilité au niveau approprié.

L'ensemble du personnel intégré au bureau de protection du secret est identifié formellement dans une note ou un registre dédié identifiant leurs signatures, actualisé autant que nécessaire.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE

2.7

2. Moyens

Pour faciliter le suivi des informations et supports classifiés, le bureau de protection du secret détient pour chaque document les informations suivantes :

Traçabilité des événements concernant les exemplaires du support d'information

Types d'évènements	Informations requises par type d'évènement
- arrivée	- numéro de référence de l'évènement
- départ	- date de l'évènement
- impression/reproduction	- référence individuelle des exemplaires
- archivage	- nom et fonction du détenteur de chaque exemplaire
- destruction	
- déclassification	
- changement de détenteur	

Modification éventuelle des données précédentes

Recherche sur les supports d'information

- détenteurs successifs d'un exemplaire
- date de création
- service émetteur

Inventaire des informations et supports classifiés

Fourniture d'états relatifs aux actions effectuées sur les supports d'information

- | | |
|---|--------------------------------|
| - historique | - procès-verbal de destruction |
| - fiche d'enregistrement | - avis de déclassification |
| - fiche de suivi | - archivage |
| - bordereau d'envoi (suivi strict des ABB') | - impression/reproduction |

3. Organisation au ministère

Au sein du ministère, suivant son positionnement hiérarchique dans la chaîne de protection du secret, un bureau de protection du secret peut être :

- un bureau principal de protection du secret (BPPS) ;
- un bureau secondaire de protection du secret (BSPS), subordonné à un BPPS ;
- un bureau de protection du secret (BPS), subordonné à un bureau secondaire de protection du secret (BSPS) ou directement au BPPS.

Il est dirigé par un officier de sécurité.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8****FORMATION ET SENSIBILISATION****Référence :**

- IGI 1300 – 3.6

Points clés

- L'officier de sécurité et l'officier de sécurité des systèmes d'information pilotent la formation des spécialistes de leur chaîne et la sensibilisation de l'ensemble du personnel.
- La formation initiale est dispensée à l'occasion de stages qualifiants. Elle est entretenue au sein de la chaîne de défense-sécurité.
- La sensibilisation initiale faite à la personne habilitée lors de la délivrance d'une décision d'habilitation donne lieu à la signature d'un engagement de responsabilité. Elle est renouvelée tout au long de l'emploi, à une fréquence régulière.

1. Formation du personnel armant les structures de sécurité

Dans le cadre de sa **formation initiale**, l'officier de sécurité suit une formation qualifiante délivrant les compétences définies dans la directive de formation de la DPID, éventuellement complétées par des compétences particulières fixées dans la PPS de la chaîne dont il relève.

Les officiers de sécurité et officiers de sécurité des systèmes d'information des personnes morales liées par contrat ou convention effectuent un stage de formation qui doit être évalué régulièrement puis accepté par l'autorité d'habilitation de la personne morale.

Le cas des officiers de sécurité des systèmes d'information, également soumis à cette obligation de formation qualifiante, est traité par ailleurs (cf. fiche 2.6 pour les officiers de sécurité des systèmes d'information des entités contractantes et PSSI-M pour les officiers de sécurité des systèmes d'information du département ministériel).

Au sein du ministère, en complément de cette formation initiale obligatoire, les personnes ayant des responsabilités particulièrement sensibles au regard de la protection du secret²⁹ et de la sécurité numérique³⁰ bénéficient d'une **formation continue** sous la responsabilité de la chaîne de défense-sécurité de l'entité à laquelle elles appartiennent.

²⁹ Officier de sécurité, officier de sécurité des systèmes d'information, personnes servant dans les bureaux de protection du secret ou en charge du suivi des informations et supports classifiés, personnes en charge de l'administration de la sécurité des systèmes numériques classifiés ou disposant de droits d'accès privilégiés à ces systèmes.

³⁰ Administrateurs, responsables de la sécurité des systèmes d'information, correspondants sécurité des systèmes d'information, etc.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8****2. Sensibilisation initiale du personnel habilité**

L'ensemble du personnel habilité est sensibilisé aux enjeux, aux risques et à ses responsabilités en matière de protection du secret de la défense nationale. La sensibilisation initiale s'appuie sur les textes réglementaires en vigueur et est officialisée par la signature d'un **engagement de responsabilité** (voir fiche 3.5). Cette sensibilisation doit intégrer les enjeux, risques et responsabilités liés à la sécurité numérique.

Cette sensibilisation est organisée par l'officier de sécurité et l'officier de sécurité des systèmes d'information. La sensibilisation précise à cette occasion les règles de gestion des informations et supports classifiés, les obligations de confidentialité. En particulier, il est rappelé que le personnel habilité ne peut pas se prévaloir de sa qualité de personne habilitée en dehors de l'exercice de ses fonctions ou de l'accomplissement de sa mission.

Les **responsables de sécurité** (officier de sécurité, officier de sécurité des systèmes d'information, etc.) reçoivent, quant à eux, de leur poste de rattachement RSD compétent, une information générique en matière de protection du secret adaptée à leur situation (responsabilités futures, outils, contacts).

3. Sensibilisation des autres personnes

Une sensibilisation régulière est la clé de voûte de la prévention en matière de protection, notamment celle du secret de la défense nationale et des systèmes numériques. Elle permet de convaincre de la nécessaire adhésion à la politique de sécurité. Elle est organisée par l'officier de sécurité et l'officier de sécurité des systèmes d'information, appuyés par le personnel des bureaux de protection du secret et des chaînes de sécurité numérique.

Les sensibilisations découlent d'une politique de sensibilisation mise en place au niveau du site, adaptée aux profils des personnes à sensibiliser, prenant en compte les risques identifiés dans l'analyse de risques et évolutive en fonction de la menace et des incidents récents. Leur efficacité repose sur la présentation de cas concrets étayés et commentés. Elles peuvent prendre la forme d'une conférence, d'un face-à-face, d'un document, voire d'un e-learning.

Ces sensibilisations peuvent notamment évoquer les thématiques suivantes :

- les risques d'investigations ou d'approches par des individus ou des organisations étrangères ;
- les dispositions législatives et réglementaires en vigueur (code pénal, code de la défense, instructions interministérielles et ministérielles, présente instruction, etc.) ainsi que les accords et règles internationales applicables ;
- la politique de protection du secret, y compris celle des systèmes d'information de l'organisme ;
- les bonnes pratiques à mettre en œuvre dans l'environnement de travail et celles relatives à la sécurité informatique appliquées aux systèmes d'information ;

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8**

- les mesures à prendre en cas de compromission ainsi qu'en cas d'incident affectant la sécurité d'un système numérique.

La sensibilisation à la sécurité numérique s'adresse à tout public. Elle s'appuie sur des cas concrets d'attaque ou de failles relevées et indique les conséquences de ces dernières. Elle vise à améliorer l'hygiène informatique de tous.

La sensibilisation à la sécurité numérique donne les mesures et les pratiques à adopter pour diminuer le risque. Elle aborde différents sujets de sécurité numérique en adéquation avec les vecteurs de menaces du moment (supports numérique, « *malwares* », réseaux sociaux, *smartphone*, « *cloud* », etc.).

La sensibilisation aux risques de compromission s'adresse au personnel habilité. Elle consiste en un rappel de la politique de protection du secret (y compris celle des systèmes numériques de l'organisme), des obligations réglementaires, des procédures à respecter à tous les stades de vie des informations et supports classifiés et du risque pénal et contractuel encouru, des mesures à prendre en cas de compromission, ainsi qu'en cas d'incident sur un système numérique conduisant à une compromission du secret. Elle développe notamment les situations de compromission potentielles au cours de périodes de vulnérabilité particulières (déménagements, restructurations, etc.).

La sensibilisation préalable à un déplacement à l'étranger : l'officier de sécurité effectue une sensibilisation générique périodique auprès de l'ensemble des personnes habilitées ou ayant accès à des informations et supports sensibles ou protégés par la mention *Diffusion Restreinte* concernant les voyages à l'étranger pour des raisons professionnelles ou personnelles.

Lorsqu'une personne habilitée est amenée à se rendre pour des raisons professionnelles hors du territoire national³¹, dans un pays que l'organisme considère comme présentant des risques particuliers pour son activité, elle avertit son officier de sécurité afin qu'il la sensibilise de manière spécifique. En cas de déplacements fréquents, la sensibilisation n'est pas systématique avant chaque déplacement si le niveau de menace et les mesures de sécurité n'ont pas évolué. L'officier de sécurité des systèmes d'information s'assure que des mesures de sécurité numérique adaptées sont prises dans le cadre de ce déplacement (mise en place de moyens spécifiques à la mission ne comprenant que les informations nécessaires à la mission, etc.).

Pour les déplacements à l'étranger, il convient de respecter les règles suivantes :

- se munir uniquement des pièces d'identité et des documents techniques, notes ou fichiers informatiques strictement indispensables à la mission ou au déplacement, à l'exclusion de tout autre, tels que des carnets d'adresses, des notes etc., susceptibles d'être photographiés ou même confisqués ;
- seuls sont autorisés les cadeaux remis lors d'échanges protocolaires, à l'exclusion de tout autre cadeau remis par des personnes inconnues ;

³¹ De surcroît, le militaire demande l'autorisation à sa chaîne hiérarchique en initiant une demande de séjour à l'étranger (cf. fiche 9.6).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8**

- en cas d'incident lors d'un déplacement ou d'événement de toute nature, en informer immédiatement les services diplomatiques français sauf consigne contraire de son organisme ;
- le stationnement à proximité des casernes ou d'autres établissements des forces armées de certains pays, la circulation sur un itinéraire non explicitement autorisé de même que la prise de vue d'installations militaires ou gouvernementales à l'étranger sont prohibés ;
- le transport de documents classifiés s'effectue dans le cadre des règles présentées dans la fiche 7.8 de la présente instruction ;
- les postes informatiques portables et les documents de travail ne doivent jamais rester sans surveillance. Ils peuvent faire l'objet de directives spécifiques (SMOBI, etc.).

La sensibilisation à la sécurité économique s'adresse particulièrement au personnel des organismes contractants du ministère (entreprises privées, etc.).

Elle met en exergue les menaces pouvant obérer la capacité de production de l'organisme et l'incidence économique résultante. Elle s'attache à développer les risques induits par les comportements humains à risques, dans l'emploi de nouvelles technologies ou dans l'application des règles établies. Elle présente les risques d'atteinte à l'image et à la notoriété.

Sensibilisation aux bonnes pratiques personnelles³² sur les réseaux sociaux³³

L'usage désormais courant des réseaux sociaux accroît les risques de communication, volontaire ou non, d'informations professionnelles et personnelles sensibles. Le respect des dispositions énoncées précédemment impose des pratiques de bon sens sur les réseaux sociaux. Elles peuvent être rappelées au personnel par l'OS de l'entité :

- séparer sa vie professionnelle de sa vie personnelle ;
- sécuriser au maximum ses comptes et profils (utilisation de pseudonymes, d'avatars, etc.)³⁴ ;
- maîtriser l'utilisation des réseaux sociaux et le contenu de ses publications (configuration en mode privé, accès aux contacts autorisés) ;
- porter une attention particulière aux visages, badges, bandes patronymiques et arrière-plans de ses photos/vidéos (l'appartenance au ministère de la défense ne doit pas être identifiable) ;
- sur les profils professionnels :
 - o les contenus ne doivent pas être trop détaillés (pas d'affectation, de spécialité détaillée, etc.) ;

³² Ces bonnes pratiques ne concernent pas les actions de communication organisées par l'organisme.

³³ Un guide du bon usage des réseaux sociaux est disponible sur le site du ministère (Cf. <https://www.defense.gouv.fr/aides-demarches/guide-du-bon-usage-reseaux-sociaux>).

³⁴ Pour en savoir plus, des guides sont disponibles sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.8**

- pour les agents publics, préférer l'appellation « agent de la fonction publique » à une appellation plus détaillée traduisant le statut ;
- ne pas diffuser d'informations privées (adresse, téléphone, etc.) ;
- respecter le cadre particulier des opérations :
 - ne pas évoquer ses missions ;
 - ne pas utiliser de géolocalisation ;
 - ne pas diffuser de photos ou vidéos pouvant révéler des localisations, des éléments de mission ou la nature des équipements employés ;
- ne pas identifier les autres personnels du même employeur ;
- n'utiliser que les outils informatiques (messageries instantanées, travail collaboratif, partage d'information, etc.) fournis ou explicitement autorisés par l'organisme. En particulier :
 - l'échange d'informations sensibles, *Diffusion Restreinte* ou classifiées via des outils non homologués est interdit,
 - l'utilisation d'outils publics de communication (messageries ou réseaux sociaux par exemple) pour l'échange de données professionnelles est interdite pour le personnel du ministère de la défense, sauf autorisation explicite du chef d'entité concerné sur un périmètre et des usages clairement définis.

Il est également important de sensibiliser l'entourage en particulier sur les principes suivants :

- il n'existe aucun moyen certain de s'assurer de la suppression d'une information une fois publiée sur Internet ;
- les données publiées peuvent être récupérées et réemployées par des acteurs malveillants ;
- toute publication est une porte d'entrée pour obtenir des informations nécessaires à la préparation d'une action malveillante (surveillance, localisation, menaces, tentative de subversion, etc.). Il faut donc expliquer à son entourage ce qu'il peut et ne peut pas faire ;
- Il est nécessaire d'encourager l'entourage à respecter la discrétion de l'agent (ne pas identifier/tagguer l'agent, ne pas faire état de sa fonction, etc.).

Le défaut d'informations d'une ou plusieurs de ces mises en garde et bonnes pratiques n'exonère toutefois pas l'agent habilité du respect de ses devoirs attachés à son habilitation et décrits dans l'engagement de responsabilité, signé par lui.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.9****INSPECTIONS, AUDITS ET CONTRÔLES DES PERSONNES MORALES DÉTENANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS ET DES SYSTÈMES NUMÉRIQUES NÉCESSAIRES À L'EXÉCUTION DU CONTRAT****Référence :**

- IGI 1300 – 2.3.3

Points clés

- Des contrôles internes et externes permettent de vérifier la bonne application des mesures de protection du secret et de la sécurité numérique.
- L'officier de sécurité de niveau 1 et l'officier de sécurité des systèmes d'information (l'officier central de sécurité des systèmes d'information le cas échéant) fixent respectivement dans la politique de protection du secret et la politique de sécurité numérique de l'organisme les obligations en matière de contrôle interne.
- Des inspections, contrôles ou audits des personnes morales ayant accès à des informations ou supports classifiés et mettant en œuvre des systèmes numériques soumis à la présente instruction sont ordonnés périodiquement par le fonctionnaire de défense et de sécurité ou par le fonctionnaire de sécurité des systèmes d'information. Ils bénéficient de l'appui, si nécessaire, des services compétents en matière de protection physique et de sécurité des systèmes d'information, en particulier la DRSD, mais également des autres organismes de contrôle du ministère de la défense (COMCYBER, DGA, etc.).
- Le contrôle externe est structuré en fonction des domaines par différentes réglementations qui font intervenir des acteurs distincts pour les domaines de la protection du secret, des informations sensibles et *Diffusion Restreinte*, des systèmes numériques soumis à la présente instruction. Interviennent notamment :
 - le contrôle du représentant du pouvoir adjudicateur (RPA), de l'autorité d'habilitation, de l'autorité de sécurité déléguée et du service enquêteur concerné (cf. fiche 4.13) auxquels les entités liées par contrat ou convention ont l'obligation de se soumettre ;
 - les inspections du SGDSN, notamment pour les classifications spéciales et les informations relevant de l'OTAN et de l'UE ;
 - les inspections conduites par l'IAN et l'ANSSI sur les domaines de leur compétence.

Les inspections, audits et contrôles ont pour objet la vérification de :

- la capacité des personnes morales à maîtriser les risques et réagir efficacement face aux menaces identifiées ;
- la conformité des entités aux dispositifs de protection et à la réglementation définie dans les documents de référence.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.9**

Les inspections, audits et contrôles sont des missions d'expertise dont le périmètre est défini par le commanditaire, interne ou externe à l'organisme. Cette action recouvre des opérations de vérification, de contrôle et d'évaluation répondant à des exigences normatives et réglementaires fixées notamment par l'IGI 1300. Ces missions se traduisent par un diagnostic de l'organisation et l'identification de vulnérabilités, faiblesses ou de non-conformité afin d'apporter les recommandations permettant de définir et de mener toutes actions correctives nécessaires et des actions de progrès. Elles donnent lieu à la rédaction et diffusion d'un rapport. Les inspections, audits et contrôles diffèrent vis-à-vis des paramètres fixant le cadre d'actions de ces missions que sont : le commanditaire, le périmètre audité et le référentiel.

1. Contrôle interne au sein des chaînes de protection du secret et de sécurité numérique

Les contrôles internes, conduits directement par les personnes morales, constituent l'action de contrôle essentielle en matière de protection du secret et de sécurité numérique pour l'ensemble des sites et entités.

Cette action est à la charge des chaînes de protection du secret et de sécurité numérique au sein des états-majors, directions et services et des personnes morales contractantes ou liées par convention. Sous l'autorité du responsable d'organisme (cf. fiche 2.4), les contrôles sont proposés et menés ou pilotés par les officiers de sécurité et officiers de sécurité des systèmes d'information, chacun dans leur domaine respectif.

L'officier de sécurité de niveau 1 (ou l'officier central de sécurité, officier de sécurité de groupe ou de *holding*, pour les personnes morales contractantes) est responsable du contrôle de la chaîne de protection du secret dont il est l'autorité fonctionnelle³⁵. Ces contrôles sont réalisés selon une périodicité maximale de trois ans. Ils donnent lieu à un procès-verbal suivi de l'élaboration d'un plan d'actions, dont l'avancement est suivi dans un bilan annuel.

L'officier de sécurité des systèmes d'information (l'officier central de sécurité des systèmes d'information le cas échéant) est responsable du contrôle de la chaîne de sécurité numérique dont il est l'autorité fonctionnelle³⁶. Ces contrôles sont réalisés avec une périodicité adaptée aux évolutions d'organisation, des périmètres de responsabilité et de personnels des chaînes concernées. Ces contrôles donnent lieu à un procès-verbal suivi de l'élaboration d'un plan d'actions, dont l'avancement est suivi dans un bilan annuel.

³⁵ Pour effectuer ses contrôles *in situ*, il lui est recommandé de s'appuyer sur une grille d'évaluation des vulnérabilités constatées dont le modèle est à adapter en fonction des spécificités du site.

³⁶ Ces contrôles ne sont pas des contrôles de sécurité des systèmes numériques. L'officier de sécurité des systèmes d'information peut employer une méthode analogue à celle de l'officier de sécurité afin de permettre au responsable d'organisme de consolider une vision complète de l'état de ses chaînes de sécurité.

TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN ŒUVRE**2.9****2. Contrôle externe**

Les organismes relevant du département ministériel, les établissements publics sous tutelle du ministère de la défense et les organismes liés par contrat ou convention à ce dernier sont soumis aux inspections du service enquêteur.

Les inspections sont soit planifiées, soit conduites de manière inopinée à la diligence du ministre ou du directeur du service enquêteur. L'entité menant un contrôle peut demander à l'entité contrôlée une fiche signalétique synthétisant des informations sur la sécurité de l'entité et ses activités.

Les rapports d'inspection utilisent des critères communs d'appréciation du niveau de sécurité afin de permettre la tenue à jour de tableaux de bord ministériels.

À réception du rapport d'inspection, l'entité inspectée dispose de six mois pour rendre compte des mesures correctives engagées sur son site. Ces contrôles donnent lieu à un procès-verbal suivi de l'élaboration d'un plan d'actions, dont l'avancement est suivi dans un bilan annuel effectué par l'organisme contrôlé.

Des audits peuvent être demandés par la chaîne hiérarchique dans les domaines relevant de sa compétence.

Pour les entités contractantes ou liées par convention relevant de leurs périmètres³⁷, la DGA, comme autorité d'habilitation et le fonctionnaire de sécurité des systèmes d'information, comme autorité de sécurité déléguée et autorité contractante et tête de chaîne de sécurité numérique planifient, en coordination avec le service enquêteur, et conduisent des audits de sécurité de défense et des systèmes d'informations. L'entité auditée dispose d'un délai de six mois pour remettre un plan d'action qui sera suivi régulièrement. À la suite de l'alerte de tiers, d'un incident de sécurité, ou sur demande d'une autorité, l'autorité d'habilitation de la personne morale peut réaliser, le cas échéant de manière inopinée, des contrôles.

3. Cas particuliers : Contrôle gouvernemental de la dissuasion et TS classification spéciale

La protection du secret et la sécurité numérique dans le cadre du contrôle gouvernemental de la dissuasion (CG) font l'objet de mesures de contrôle ou d'inspections supplémentaires détaillées dans des instructions spécifiques.

Des contrôles et des inspections sont organisés périodiquement par le SGDSN pour vérifier l'application, par les organismes émettant, recevant, traitant ou conservant des informations et supports classifiés de niveau *Très Secret* classification spéciale, des

³⁷ Toutes les personnes morales contractant avec le ministère hors DGSE. La DGSE planifie et conduit seule ou en coordination avec la DRSD des audits de sécurité de défense et des systèmes d'informations au titre de son rôle d'autorité d'habilitation et d'autorité contractante.

**TITRE 2 : STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN
ŒUVRE****2.9**

instructions et des directives relatives à la protection du secret. Le SGDSN propose toutes mesures propres à améliorer les conditions générales de sécurité. Les rapports de synthèse incluant les mesures préconisées pour rectifier les déficiences constatées et leur planification sont adressés aux personnes morales responsables des entités contrôlées et au ministre de la défense. En cas d'anomalies constatées, le SGDSN en informe la DPID. Il peut saisir la direction générale de la sécurité intérieure sous le contrôle et la direction de l'autorité judiciaire, sans préjudice de la dénonciation auprès du procureur de la République.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES

INTRODUCTION : PROCESSUS D'HABILITATION DU PERSONNEL

Référence :

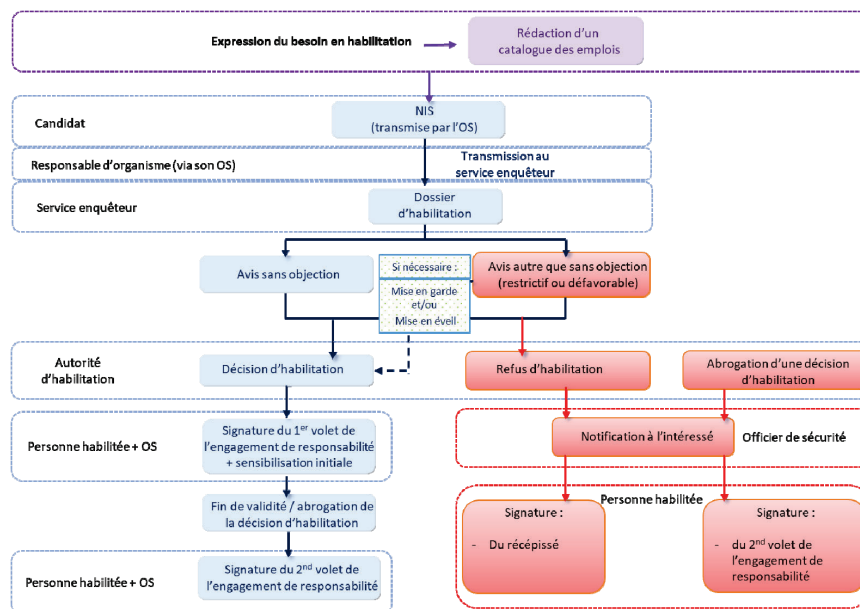
- IGI 1300 – chapitre 3

Point clé

L'accès aux informations et supports classifiés est subordonné à l'habilitation du personnel concerné et à son besoin d'en connaître.

En application du code de la défense³⁸, « *Sauf exception prévue par la loi, nul n'est qualifié, pour connaître des informations ou supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin, au regard du catalogue des emplois justifiant une habilitation, établi selon les modalités précisées par arrêté du Premier ministre, de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission* ».

Le processus d'habilitation au sein du ministère, également appliqué aux établissements publics qui lui sont rattachés, suit un cheminement rigoureux décrit dans le schéma³⁹ ci-dessous et précisé dans les fiches 3.1 à 3.6.



³⁸ Article R.2311-7 du code de la défense.

³⁹ Ce schéma n'est pas applicable aux procédures d'habilitation pour l'accès au TRES SECRET CLASSIFICATION SPECIALE, au COSMIC TOP SECRET et au TRES SECRET UE, ni pour les habilitations des personnes de droit étranger.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.1**CATALOGUE DES EMPLOIS****Références :**

- IGI 1300 – 3.1.2
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Le catalogue des emplois établit pour un niveau de classification la liste des postes pour lesquels le besoin d'en connaître est avéré et une procédure d'habilitation doit être engagée.
- L'appréciation du besoin d'en connaître doit être rigoureuse et mesurée au plus juste. Le catalogue est révisé annuellement par les autorités d'emploi.
- Les personnes morales de droit privé exécutant un contrat ou une convention soumis au respect de la protection du secret doivent être habilitées et détenir également un catalogue des emplois.

1. Généralités

L'appréciation du besoin d'en connaître est fondée sur le principe selon lequel une personne ne peut avoir accès à des informations et supports classifiés que dans la mesure où l'exercice de sa fonction ou l'accomplissement de sa mission l'exige.

Cette appréciation du besoin d'habilitation doit être rigoureuse et mesurée. Il convient ainsi d'éviter la solution de facilité consistant, faute de vouloir discriminer ceux qui ont véritablement besoin de connaître des informations classifiées, à demander des habilitations pour tout le personnel d'un état-major, d'un service, d'un organisme, d'une unité ou d'une formation, d'une promotion d'élèves ou d'un stage. Le besoin d'en connaître est attesté par la demande d'habilitation, jointe à la notice individuelle de sécurité (NIS), incluse dans le dossier d'habilitation (cf. IGI 1300 - annexes 5 et 7) dans lequel figure, en particulier, le numéro d'inscription au catalogue des emplois.

2. Procédure

L'autorité d'emploi, qu'il s'agisse d'un service du ministère de la défense, d'un établissement public ou d'une personne morale liée par contrat ou convention avec ce dernier, établit pour chaque nature et niveau d'habilitation un catalogue des emplois⁴⁰ qui précise, *via* l'octroi d'un numéro de poste, les fonctions et missions impliquant nécessairement⁴¹ l'accès à des informations et supports classifiés de niveau *Secret* et

⁴⁰ Peuvent coexister au sein d'un organisme des catalogues NATO SECRET (SO) et SECRET UE (SUE) par exemple.

⁴¹ Les emplois nécessitant une décision d'accès aux articles contrôlés de la sécurité des systèmes d'information (DACSSI) pour la manipulation d'articles contrôlés de la sécurité des systèmes d'information imposent également de détenir une habilitation en prérequis à celle-ci.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.1

Très Secret ainsi que les nom et prénom des personnes physiques les occupant. Une copie du catalogue des emplois est adressée à l'autorité d'habilitation.

Les demandes d'habilitation sont établies en référence au catalogue des emplois. Au cours de la procédure, l'officier de sécurité vérifie l'inscription de la fonction concernée dans le catalogue des emplois correspondant. Il examine, à titre exceptionnel, le bien-fondé de la demande lorsque l'emploi ne figure pas au catalogue et le modifie en conséquence.

Après analyse de l'officier de sécurité, le catalogue est révisé annuellement par les autorités d'emploi⁴² et à l'occasion de chaque réorganisation de service. Il peut faire l'objet d'un contrôle par l'autorité d'habilitation ou par le haut fonctionnaire correspond de défense et de sécurité afin de vérifier, notamment, si les titulaires des fonctions répertoriées ont effectivement accès à des informations et supports classifiés pour le niveau concerné.

Tout agent occupant ou envisageant d'exercer une fonction ou d'accomplir une mission requérant un accès à des informations et supports classifiés est tenu de se soumettre à une procédure d'habilitation. Tout refus entraîne *de facto* l'impossibilité pour l'intéressé d'occuper cet emploi.

Dans le cas où un organisme sollicite un réserviste citoyen pour une mission d'expertise, une lettre de mission doit être co-signée par le responsable d'organisme et le réserviste. Elle doit détailler les obligations particulières de discrétion professionnelle et de discipline auxquelles ce dernier est soumis, sa chaîne hiérarchique d'emploi, la durée de sa mission et le niveau d'habilitation sollicité. Cette mission est ensuite inscrite au catalogue des emplois de l'organisme.

⁴² Pour les services du ministère, la période estivale est à privilégier.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.2**DEMANDE D'HABILITATION****Référence :**

- IGI 1300 – 3.2 et 3.3

Points clés

- La notice individuelle de sécurité, en format dématérialisé, doit être privilégiée par tous les candidats pour transmettre leurs demandes à l'officier de sécurité de leur organisme. Après un contrôle, sous la responsabilité de l'officier de sécurité, ce dernier l'adresse au service enquêteur⁴³.
- La demande d'habilitation est engagée lorsque la fonction est inscrite au catalogue des emplois ou lorsqu'un besoin d'accéder à des informations et supports classifiés pour des opérations est avéré.
- Exceptionnellement, la demande d'habilitation peut suivre des procédures dérogatoires à la procédure de droit commun (procédure d'urgence et procédure simplifiée). Le recours à celles-ci est dûment justifié.
- Le recours aux procédures dérogatoires (simplifiée et urgente) est prohibé pour l'habilitation des agents des services de renseignement.

1. Lancement de la procédure

Le responsable d'organisme employeur, *via* son officier de sécurité, s'assure en premier lieu que la demande d'habilitation est justifiée par le besoin d'accéder à des informations et supports classifiés pour exercer une fonction ou accomplir une mission inscrite au catalogue des emplois.

L'officier de sécurité informe ensuite le candidat des obligations induites par l'habilitation ainsi que des dispositions relatives à sa responsabilité pénale en cas de compromission. Il lui précise la procédure d'habilitation choisie.

2. Procédure de droit commun

L'officier de sécurité transmet au candidat une notice individuelle de sécurité. Ce dernier la complète sous forme informatique⁴⁴. Un exemplaire est signé par le candidat. Cette pièce officielle, dont la complétude et la cohérence sont vérifiées par l'officier de sécurité avant d'initier la demande d'habilitation, est conservée par l'employeur. Ce dernier doit être en mesure de la produire en cas de réclamation. Elle est détruite un an après la fin de validité de l'avis de sécurité émis par le service enquêteur.

Le dossier d'habilitation se compose des documents énumérés ci-dessous :

⁴³ Par dérogation au 3.3.1.1 de l'IGI 1300.

⁴⁴ Formulaire à renseigner sur le module de saisie en ligne ou à télécharger sur le site Intradef de la DRSD ou sur le site Internet armement.defense.gouv.fr pour les personnes morales contractantes.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.2

- d'un dossier d'habilitation⁴⁵ organisé en deux parties :
 - o une demande d'habilitation signée par le responsable d'organisme ou l'officier de sécurité attestant le besoin de connaître des informations et supports classifiés à un niveau donné⁴⁶ ;
 - o la notice individuelle de sécurité renseignée intégralement, datée et signée par le candidat ;
 - o une photographie récente (moins de six mois, format identique à celui demandé pour la carte nationale d'identité) numérisée. Le dossier d'habilitation au niveau S ou TS (hors classification spéciale⁴⁷) est transmis au service enquêteur *via* SOPHIA⁴⁸.

Les demandes d'habilitation au niveau TS faisant l'objet d'une classification spéciale sont transmises selon une procédure spécifique et instruites par le SGDSN, autorité d'habilitation pour ce niveau.

La procédure d'habilitation de niveau *Secret* ou *Très Secret* n'est engagée qu'au seul profit de la personne effectivement nommée dans l'emploi. L'anticipation doit être privilégiée afin de permettre une habilitation avant sa prise de fonction. Ainsi, le dossier d'habilitation constitué doit être transmis à l'autorité d'habilitation avant toute prise de poste.

3. Procédures dérogatoires à la procédure de droit commun

Ces procédures sont prohibées pour l'habilitation des agents des services spécialisés de renseignement, visés à l'article R.811-1 du code de la sécurité intérieure, à l'exception des agents nommés conformément à l'article 13 de la Constitution ou relevant du chapitre Ier du titre II du décret n° 2019-1594 du 31 décembre 2019 relatif aux emplois de direction de l'État.

Elles le sont également concernant le personnel de la DGSE et des organismes contractants qui lui sont rattachés. Ils répondent à une procédure qui est propre à cette direction.

a. Procédure d'urgence

Certaines situations qui impliquent une prise de connaissance immédiate d'informations et supports classifiés ne peuvent se satisfaire des délais de la procédure normale et justifient la mise en œuvre d'une procédure d'urgence :

- départ imminent en opération extérieure d'une personne non habilitée (OPEX) ;
- prise de fonction ou évolutions des fonctions nécessitant l'accès immédiat à des informations et supports classifiés ;
- nécessité pour des raisons de carrière (passage sous-officier de carrière, etc.) ;

⁴⁵ *Idem.*

⁴⁶ Cf. modèle : annexe 7 de l'IGI 1300.

⁴⁷ Sauf aux niveaux COSMIC TRES SECRET et TRES SECRET UE qui font l'objet d'une procédure spécifique.

⁴⁸ Les procédures d'utilisation de SOPHIA sont disponibles sur le site Intradef de la DRSD, les sites internet des états-majors, directions et services disposant d'OS de niveau 1 ou du SGDSN.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.2

- désignation d'une personne non habilitée à un stage de formation au dernier moment ou à un stage non planifié.

Dans les quinze jours ouvrables suivant sa saisine, le service enquêteur émet un avis de sécurité provisoire. La procédure de droit commun se poursuit après l'émission de l'avis de sécurité provisoire. Au regard de ce dernier, l'autorité d'habilitation peut prendre une décision d'habilitation provisoire qui expire :

- soit lorsqu'à réception de l'avis de sécurité définitif, la décision d'habilitation ou de refus d'habilitation est prise ;
- soit six mois après sa date d'émission.

Cette procédure ne remplace, ni n'interrompt la procédure normale. Elle doit être légitime, motivée par écrit sur le formulaire de demande, rester exceptionnelle et en aucun cas pallier un manque de planification des organismes demandeurs. Le service enquêteur peut refuser de traiter une telle demande s'il constate un détournement de cette procédure. Ce détournement est caractérisé notamment par une motivation stéréotypée ou lacunaire.

Pour les dossiers d'habilitation au niveau *Très Secret* classification spéciale, seul le SGDSN, au regard des éléments transmis par l'autorité compétente, peut engager une telle procédure⁴⁹.

b. Procédure simplifiée⁵⁰

La procédure simplifiée n'est pas applicable au personnel des personnes morales de droit privé exécutant des contrats ou conventions conclus au profit du ministère.

Le personnel civil et militaire du ministère de la défense peut être exceptionnellement habilité au niveau *Secret* uniquement par l'autorité d'habilitation dont il relève sans intervention du service enquêteur.

L'usage de cette procédure dérogatoire doit demeurer exceptionnel. Il est impératif de ne l'employer qu'en cas de nécessité effective et pour des habilitations d'une durée **inférieure ou égale à trois mois** (notamment les stages, vacations, formations, emplois provisoires).

Cette procédure peut être appliquée à condition que le candidat :

- ait fait l'objet d'une enquête administrative de contrôle primaire (cf. fiche 3.9), datant de moins de trois ans au moment de la décision d'habilitation et dont l'avis de sécurité est sans objection ;
- ait rempli la notice individuelle de sécurité ;
- une fois la décision d'habilitation délivrée, ait signé le premier volet de l'engagement de responsabilité.

La décision d'habilitation est notifiée à l'intéressé dans les conditions ordinaires. Le service enquêteur doit en être informé.

⁴⁹ La procédure d'urgence au sein de la DGSE diffère également de celle énoncée dans cette instruction.

⁵⁰ Cette procédure n'est pas applicable aux personnes relevant des établissements publics sous tutelle du ministère.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.2

Le responsable d'organisme employeur peut engager une procédure d'habilitation de droit commun auprès du service enquêteur.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.3

AVIS DE SÉCURITÉ

Référence :

- IGI 1300 – 3.3.1.3

Points clés

- L'enquête administrative préalable à une habilitation est menée par le service enquêteur. Elle s'achève par l'émission d'un avis de sécurité.
- L'autorité d'habilitation n'est pas tenue de suivre l'avis de sécurité émis. Elle prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier.

1. Généralités

L'avis de sécurité est une évaluation des vulnérabilités éventuellement détectées lors de l'enquête administrative. Il permet à l'autorité d'habilitation d'apprécier l'opportunité de l'habilitation du candidat, au regard des éléments communiqués et des garanties qu'il présente pour le niveau d'habilitation requis.

L'enquête administrative préalable à une habilitation est du ressort :

- de la DRSD :
 - pour le personnel civil et militaire relevant du ministère de la défense,
 - pour le personnel civil et militaire d'un établissement public sous tutelle,
 - pour les personnes morales intervenant dans le cadre de contrats au profit du ministère de la défense et leur personnel effectuant les travaux prévus par ces contrats,
 - le personnels militaire de la gendarmerie ;
- de la DGSE :
 - pour le personnel civil ou militaire qui y est affecté,
 - pour les personnes morales contractantes intervenant dans le cadre de contrats au profit de la DGSE et leur personnel effectuant les travaux prévus par ces contrats.

Les conclusions de l'avis de sécurité de la DRSD sont de trois types :

- **sans objection (SO)**, lorsque l'instruction n'a révélé aucune vulnérabilité de nature à constituer un risque pour la sécurité des informations et supports classifiés ni pour celle de l'intéressé ;
- **autres que sans objection (AQSO) :**
 - **avis restrictif**, lorsque le candidat présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations et supports classifiés auxquels il aurait accès mais que des mesures de sécurité spécifiques prises par l'officier de sécurité et, le cas échéant, une sensibilisation particulière du candidat permettraient de maîtriser. Dans ce cas, le service enquêteur recommande une procédure de mise en garde de l'employeur ou de mise en éveil de l'intéressé ou qu'il soit recouru à ces deux procédures (cf. fiche 3.4),

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.3

- **avis défavorable**, lorsque des informations précises font apparaître que le candidat présente des vulnérabilités faisant peser sur le secret de la défense nationale des risques tels qu'aucune mesure de sécurité ne permettrait de les maîtriser. Néanmoins, dans le cas où l'autorité d'habilitation ne suit pas l'avis du service enquêteur et décide d'habiliter le candidat, le service enquêteur peut recommander une procédure de mise en garde de l'employeur, de mise en éveil de l'intéressé ou qu'il soit recouru à ces deux procédures (cf. fiche 3.4).

2. Validité de l'avis de sécurité

L'avis de sécurité est émis pour un niveau donné d'habilitation. L'avis sans objection est valable pour le niveau pour lequel il a été requis et, le cas échéant, pour le niveau inférieur. Sa durée de validité ne dépasse pas celle de l'avis initial.

La durée de validité de l'avis de sécurité est fonction du niveau d'habilitation demandé. Elle ne peut excéder :

- **sept ans** pour le niveau *Secret* ;
- **cinq ans** pour le niveau *Très Secret*.

L'avis de sécurité ne constitue en soi ni une autorisation, ni un refus et ne lie pas l'autorité d'habilitation, qui prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier (nature de l'avis de sécurité, sensibilité du poste tenu par l'intéressé et tout autre élément permettant à l'autorité d'habilitation d'apprécier le degré de confiance à accorder).

3. Transmission des avis de sécurité⁵¹

Selon le cas, le service enquêteur fait parvenir à l'autorité d'habilitation :

- l'avis de sécurité sans objection ;
- un exemplaire de l'avis de sécurité restrictif ou défavorable, accompagné d'une fiche confidentielle classifiée, exposant les motifs justifiant l'avis. La fiche confidentielle est composée d'éléments qui peuvent être communiqués au candidat dans le cadre d'une mise en éveil⁵² ou à l'employeur pour une mise en garde⁵³ et d'éléments classifiés qui ne peuvent être portés qu'à la connaissance de l'autorité d'habilitation ou de son officier de sécurité.

⁵¹ Ce paragraphe ne s'applique pas à la DGSE qui dispose de ses propres procédures internes.

⁵² La mise en éveil consiste à sensibiliser le candidat à l'habilitation aux vulnérabilités révélés par l'enquête administrative (point 3.4.1.2.de l'IGI 1300).

⁵³ La mise en garde consiste à sensibiliser l'employeur aux vulnérabilités du candidat mises en exergue par l'enquête administration afin prendre les mesures de sécurité ou les précautions particulières à l'égard de l'intéressé (point 3.4.1.2.de l'IGI 1300).

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.3

Ne pouvant être reproduite, après sa communication, la fiche confidentielle est retournée par l'autorité d'habilitation au service enquêteur à des fins de conservation⁵⁴. L'autorité d'habilitation peut, en tant que de besoin, demander à nouveau communication des éléments de la fiche confidentielle :

- lorsqu'elle est chargée de mettre en garde l'autorité d'emploi ;
- en cas de changement de comportement ou de situation de l'intéressé ;
- à l'occasion de l'instruction d'une nouvelle demande d'habilitation le concernant ;
- pour l'instruction des recours gracieux ou contentieux dont la décision qu'elle a prise sur la base de l'avis de sécurité du service enquêteur peut faire l'objet.

Au terme de l'instruction de la procédure d'habilitation, l'autorité d'habilitation informe le service enquêteur de la décision prise (refus ou admission à l'habilitation) ainsi que des suites données aux recommandations.

La validité de la décision d'habilitation ne peut excéder celle de l'avis de sécurité initial.

4. Durée de conservation

L'exemplaire de l'avis de sécurité signé et retourné au service enquêteur est conservé par celui-ci sous forme numérique sans limitation de durée⁵⁵.

⁵⁴Sauf lorsque le processus est dématérialisé.

⁵⁵ Sauf lorsque le processus est dématérialisé.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.4**MISE EN ÉVEIL ET MISE EN GARDE****Référence :**

- IGI 1300 – 3.4.1.2

Points clés

- L'autorité d'habilitation peut décider, lorsque l'enquête a mis en évidence des éléments de vulnérabilité, d'accorder l'habilitation après avoir pris des précautions particulières, à savoir la mise en éveil de l'intéressé, la mise en garde de l'employeur ou les deux.
 - La mise en éveil est une sensibilisation de l'intéressé sur les éléments communicables de vulnérabilité révélés par l'enquête.
 - La mise en garde concerne exclusivement l'officier de sécurité ou son employeur. En aucun cas, la personne habilitée n'est informée de la procédure de mise en garde.

1. Généralités

L'enquête administrative effectuée par le service enquêteur se traduit par l'émission d'un avis de sécurité destiné à l'autorité d'habilitation. En cas d'avis autre que sans objection, l'autorité d'habilitation peut décider de n'accorder l'habilitation qu'après la mise en œuvre de l'une ou l'autre des mesures de sécurité suivantes :

- la mise en éveil de l'intéressé ;
- la mise en garde de l'autorité compétente ou de l'officier de sécurité de l'organisme dont relève le candidat à l'habilitation.

Les procédures de mise en garde et de mise en éveil peuvent être cumulées.

2. Procédure de mise en éveil de l'intéressé

La mise en éveil consiste à sensibiliser le candidat à l'habilitation sur les éléments communicables de vulnérabilité révélés par l'enquête⁵⁶.

En coordination avec l'autorité d'habilitation, l'officier de sécurité effectue la mise en éveil avec l'appui éventuel du service enquêteur si l'officier de sécurité le demande. La responsabilité de la mise en éveil est uniquement du ressort de l'officier de sécurité.

À l'issue de l'entretien de mise en éveil, une attestation (cf. IGI 1300 - annexe 10) est signée par l'officier de sécurité concerné, l'intéressé et par le représentant de l'autorité d'habilitation⁵⁷ puis conservée par l'autorité d'habilitation. L'habilitation n'est délivrée qu'à l'issue de la réalisation de la mise en éveil et effective à compter de la signature du

⁵⁶ Il peut s'agir par exemple de ses attaches avec l'étranger ou de diverses particularités de son environnement. Il revient au service enquêteur d'apprécier, pour chaque cas, ce qui peut constituer une vulnérabilité.

⁵⁷ Qui peut être l'officier de sécurité.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.4

volet 1 de l'engagement de responsabilité. L'autorité d'habilitation ou l'officier de sécurité informe le service enquêteur de la notification de la mise en éveil.

3. Procédure de mise en garde de l'autorité compétente

La mise en garde consiste, pour l'autorité d'habilitation, après avoir été informée par le service enquêteur et avec son concours le cas échéant, à avertir l'employeur ou son officier de sécurité des éléments de vulnérabilité révélés par l'enquête, en dehors de la présence du candidat à l'habilitation. L'autorité d'habilitation demande alors à l'autorité compétente de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si nécessaire avec le conseil du service enquêteur. Une nouvelle mise en garde peut être effectuée lors d'un changement d'employeur.

À l'issue de l'entretien de mise en garde, une attestation (cf. IGI 1300 - annexe 9) est signée par l'officier de sécurité ou l'employeur dont relève l'intéressé et conservée par l'officier de sécurité et l'autorité d'habilitation. Cette dernière en informe le service enquêteur.

L'habilitation n'est délivrée qu'après la mise en garde de l'autorité compétente et devient effective après signature du volet 1 de l'engagement de responsabilité par le candidat.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.5**DÉCISION D'HABILITATION OU DE REFUS D'HABILITATION****Références :**

- Arrêté du 21 mars 2012 modifié portant délégation des pouvoirs du ministre de la défense en matière de décisions d'habilitation à connaître des informations et supports couverts par le secret de la défense nationale
- IGI 1300 – 3.4

Points clés

- La décision d'habilitation est prise par l'autorité d'habilitation compétente.
- Elle s'appuie notamment sur l'avis de sécurité émis par le service enquêteur⁵⁸.
- Lors de la notification de la décision d'habilitation à l'intéressé, ce dernier signe le 1^{er} volet de l'engagement de responsabilité.
- Un refus d'habilitation n'a pas à être motivé.

1. Prise de décision

À l'issue de l'enquête administrative pour le renseignement et la sûreté, le service enquêteur émet un avis de sécurité (cf. fiche 3.3) à destination de l'autorité d'habilitation sur lequel celle-ci s'appuie notamment pour prendre sa décision. Les conclusions de l'avis de sécurité ne lient pas l'autorité d'habilitation. L'autorité d'habilitation peut établir une décision d'habilitation (cf. annexes 2 et 3) ou de refus (cf. annexes 5 et 6), qu'elle adresse via son officier de sécurité au responsable d'organisme employeur.

En présence d'un avis de sécurité sans objection, l'autorité d'habilitation peut établir une décision d'habilitation (cf. annexes 2 et 3). Elle informe l'officier de sécurité de l'organisme employeur. Les décisions sont conservées par ce dernier.

En présence d'un avis de sécurité restrictif ou défavorable, l'autorité d'habilitation peut décider ou non de prononcer l'admission. Pour éclairer sa décision, elle peut réunir une commission regroupant en particulier l'officier de sécurité et l'employeur de l'intéressé, lorsqu'il diffère de l'autorité d'habilitation afin d'évaluer ses vulnérabilités et les mesures compensatrices à mettre en œuvre.

a. Premier cas : l'autorité d'habilitation prononce l'admission

Dans la circonstance dans laquelle l'autorité d'habilitation souhaite accorder l'habilitation sollicitée :

- elle peut demander une mise en éveil de l'intéressé ou effectuer une mise en garde de l'employeur (cf. fiche 3.4) et étudie avec ce dernier et le service enquêteur, le cas échéant, les mesures de sécurité adéquates ;

⁵⁸ À l'exception de la procédure simplifiée qui ne concerne que le personnel du ministère (cf. fiche 3.3 paragraphe 2.b).

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.5

- elle réceptionne l'attestation de bon déroulement de cette ou ces procédures (IGI 1300 - annexes 9 et 10) ;
- elle donne son accord aux mesures de sécurité envisagées localement ;
- elle établit une décision d'habilitation.

L'officier de sécurité informe alors le responsable d'organisme employeur et procède à la notification de la décision d'habilitation. À ce titre, il fait signer le premier volet de l'engagement de responsabilité (cf. annexe 4). Cette notification doit être assortie d'une sensibilisation aux obligations particulières imposées par l'accès à des informations et supports classifiés (cf. fiche 2.8).

En revanche, la décision d'habilitation et l'avis de sécurité ne sont pas communiqués à l'agent habilité.

b. Deuxième cas : l'autorité d'habilitation prononce un refus d'habilitation

L'autorité d'habilitation établit une décision de refus (cf. annexes 5 et 6) et l'adresse au responsable d'organisme employeur.

La décision de refus est notifiée et remise à l'intéressé lors d'un entretien (cf. IM 900 – annexes 7 et 8). Elle n'a pas à être motivée ⁵⁹ mais comprend la mention des délais et voies de recours contentieux.

L'officier de sécurité lui remet un récépissé de notification de la décision de refus d'habilitation (cf. IM 900 - annexes 7 et 8). Un exemplaire, daté et signé par l'intéressé, est conservé par l'autorité d'habilitation. Une copie de la décision est adressée au service enquêteur.

Si l'autorité d'habilitation décide ultérieurement d'accorder l'habilitation, après l'avoir refusée dans un premier temps, elle doit en informer le service enquêteur.

c. Troisième cas : l'autorité d'habilitation prononce une habilitation temporaire.

La décision d'habilitation temporaire ne s'applique pas à la personne morale de droit privé ni aux personnes physiques travaillant pour le compte de cette dernière dans le cadre d'un contrat prévoyant l'exécution de travaux classifiés.

L'autorité d'habilitation peut également décider d'accorder une décision d'habilitation temporaire, à l'issue d'une procédure d'habilitation de droit commun (cf. IGI 1300, 3.3.1) à un agent de l'État ou d'un de ses établissements publics lorsque l'intéressé fait l'objet d'une habilitation au niveau *Secret* pour lequel il est inscrit au catalogue des emplois et qu'il a besoin, de façon ponctuelle, d'accéder à des informations et supports classifiés au niveau *Très Secret*, hors classification spéciale.

Cette décision, non renouvelable, est valable pour une durée maximale de trois mois, à l'exception des décisions délivrées aux militaires pour l'accomplissement de leur

⁵⁹ Article L.211-2 du code des relations entre le public et l'administration.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.5

mission en opération intérieure ou extérieure, qui sont valables la durée de la projection. L'autorité d'habilitation est tenue d'en informer le service enquêteur.

2. Durée de la décision

La durée de validité de la décision ne peut en aucun cas excéder la durée de validité de l'avis de sécurité. Elle peut, en revanche, être plus courte :

- si la décision d'habilitation le prévoit au regard des vulnérabilités qui auront été portées à sa connaissance (avis AQSO) ou compte tenu de la mission que l'agent aura à exercer ;
- en cas de procédure d'urgence (six mois à compter de son émission, cf. fiche 3.2).

Chaque décision est émise pour un poste, une mission ou une fonction. Elle est donc caduque dès que la personne cesse l'activité pour laquelle l'habilitation a été accordée.

3. Communication de la décision

Une personne titulaire d'une décision d'habilitation ne peut en faire état ni révéler son niveau d'habilitation sauf si la communication de ces informations est nécessaire à l'exercice de ses fonctions ou à l'accomplissement d'une mission pour lesquelles elle a été habilitée.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.6**GESTION ET FIN DE L'HABILITATION****Référence :**

- IGI 1300 – 3.5.1 à 3.5.8

Points clés

- La validité d'une décision ne peut excéder la validité de l'avis de sécurité émis pour un niveau donné d'habilitation (hors disposition spécifique du renouvellement).
- Une décision d'habilitation peut être abrogée à tout moment par l'autorité d'habilitation.
- Lorsqu'une personne cesse d'être habilitée, elle est tenue de ne pas divulguer les informations classifiées dont elle a eu connaissance pendant l'exercice de ses fonctions ou l'accomplissement de sa mission.

En complément du catalogue des emplois, le responsable d'organisme employeur, *via* son officier de sécurité, fait tenir, pour chaque niveau de classification, un répertoire des dossiers d'habilitation en cours d'instruction et de suivi des habilitations en cours de validité. Ce dernier facilite la gestion des habilitations et permet de retrouver, de manière très rapide, les différentes informations nécessaires sur les personnes habilitées (date d'émission de la demande, niveau et nature d'habilitation, fonction ou mission du candidat, durée de validité, etc.).

Dans les services ministériels, l'autorité d'habilitation archive la décision d'habilitation ou de refus d'habilitation.

En cas de nécessité, quel que soit l'organisme, un certificat de sécurité (cf. IGI 1300 - annexe 14) peut être délivré par l'autorité d'habilitation ou par l'officier de sécurité de l'organisme de l'intéressé pour une mission ou pour une période déterminée.

1. Durée de validité des décisions d'habilitation

L'habilitation arrive à échéance au terme fixé dans la décision et, en tout état de cause, à la cessation des fonctions au titre desquelles elle a été accordée, quand bien même la date de fin de validité inscrite sur la décision n'est pas échue.

Elle peut être émise pour une durée inférieure à la durée initiale de validité de l'avis de sécurité mais ne peut l'excéder (cf. fiche 3.5).

2. Conservation des décisions

Les décisions d'habilitation sont conservées par l'autorité d'habilitation pendant leur durée de validité et un an au-delà, à l'exception de celles rendues au niveau *Très Secret* classification spéciale, dont les modalités de gestion sont définies selon des directives spécifiques. Les décisions d'habilitation ne sont en aucun cas remises aux intéressés ni reproduites.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.6

Les données relatives à l'identité des personnes habilitées et aux éléments techniques de gestion des dossiers d'habilitation sont conservées pour une durée d'un an après la fin de validité de l'avis de sécurité émis par le service enquêteur.

3. Certificat de sécurité

Chaque fois qu'il est nécessaire, pour l'accomplissement d'une mission, de présenter un document attestant une habilitation au niveau requis, un certificat de sécurité (cf. IGI 1300 - annexe 14) est délivré à l'intéressé par l'autorité d'habilitation ou l'officier de sécurité de l'organisme auquel il appartient au vu de la décision d'habilitation effectivement détenue. La durée de validité de ce document, limitée à un an au maximum, doit être précisée et, en tout état de cause, ne peut dépasser celle de l'habilitation correspondante⁶⁰.

À la fin de validité du certificat et au terme de la mission, l'intéressé procède ou fait procéder à sa destruction.

4. Renouvellement des habilitations

Le renouvellement de l'habilitation, pour les mêmes fonctions, est demandé dans un délai d'un an au plus tôt à trois mois au plus tard avant la date d'expiration de la validité de l'habilitation initiale. Si cette disposition est respectée, un certificat de sécurité peut être établi en reprenant les références de la décision dont la durée de validité a été tacitement prorogée pendant les douze mois qui suivent son expiration.

La procédure est mise en œuvre dans les mêmes conditions que la demande initiale.

5. Changement de situation de la personne habilitée et révision de l'habilitation

- a. La personne habilitée doit informer sans délai l'officier de sécurité, pendant toute la durée de son habilitation, de tout changement affectant sa vie personnelle (concubinage, pacte civil de solidarité, mariage, séparation, etc.), professionnelle ou géographique (lieu de domicile ou de résidence).
- b. Il lui est également signifié qu'elle doit l'informer de toute relation suivie, dépassant le cadre professionnel, avec un ou plusieurs ressortissants étrangers et de le consigner dans une notice individuelle de sécurité transmise à son officier de sécurité.

L'officier de sécurité lui fait alors remplir une notice individuelle de sécurité et la transmet au service enquêteur.

⁶⁰ Pour le personnel français affecté (et non sous contrat) dans un état-major ou un organisme de l'OTAN ou de l'UE, une attestation d'habilitation peut être éditée par l'officier de sécurité de l'élément de soutien national (ESN) ou la représentation militaire française (RMF) pour une durée couvrant l'affectation du personnel et une éventuelle prolongation de cette durée d'une année au maximum. Cette attestation d'habilitation n'est éditée que dans le but de permettre au personnel l'accès aux sites et installations relevant de l'organisation internationale dans laquelle il est affecté, en conformité avec les règles de sécurité de cette organisation. Si un avis de sécurité AQSO est émis au cours de l'affectation (suite à une révision de l'avis de sécurité à la demande de l'officier de sécurité ou en cas de changement de situation personnelle par exemple), la durée de cette attestation d'habilitation peut être revue par l'officier de sécurité ou le responsable de l'ESN ou de la RMF. Il ne remet pas en cause la durée d'un an au maximum d'un certificat de sécurité délivré pour une mission.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.6

Ce changement de situation peut entraîner une révision du dossier d'habilitation et l'émission d'un nouvel avis de sécurité.

- c. Si une vulnérabilité nouvelle est portée à la connaissance de l'autorité d'emploi, celle-ci peut décider de lancer une procédure de révision de la décision d'habilitation.
- d. Si une vulnérabilité nouvelle est portée à la connaissance du service enquêteur, celui-ci peut décider de lancer une procédure de révision de l'avis de sécurité.

6. Portabilité de l'avis de sécurité en cas de changement de fonction ou d'affectation

Lorsqu'une personne habilitée change de fonction ou d'affectation, son habilitation pour le poste initial devient caduque⁶¹. Une autre décision d'habilitation, demandée par le nouvel employeur, peut être prise, si la nouvelle affectation l'exige, sur la base de l'avis de sécurité en cours. Un nouveau dossier d'habilitation est constitué par l'officier de sécurité et composé de la demande justifiée par ce dernier et d'une notice individuelle de sécurité à nouveau renseignée par le candidat. L'officier de sécurité analyse la notice et transmet le dossier au service enquêteur s'il constate un changement de situation ou une potentielle vulnérabilité au regard du poste que le candidat sera amené à occuper, en vue d'éclairer la décision future de l'autorité d'habilitation.

En cas de changement d'autorité d'habilitation, l'officier de sécurité de l'organisme quitté informe la nouvelle autorité d'habilitation, à sa demande, qu'un avis de sécurité est en cours de validité. L'autorité d'habilitation de l'organisme quitté lui transmet alors une **attestation d'avis de sécurité**⁶² (cf. IGI 1300 - annexe 15) mentionnant notamment la nature de l'avis de sécurité (SO ou AQSO) ainsi que sa fin de validité. Si l'avis est AQSO, la nouvelle autorité d'habilitation doit, pour prendre sa décision, demander au service enquêteur à connaître les motifs qui l'ont justifié. L'autorité d'habilitation peut être conseillée par l'officier de sécurité et l'employeur du candidat pour prendre sa décision.

7. Abrogation de la décision d'habilitation

L'habilitation peut être abrogée à tout moment, à l'occasion d'une demande de renouvellement ou de révision, quand l'intéressé ne remplit plus les conditions nécessaires à sa délivrance. Cela peut être le cas lorsque des éléments de vulnérabilités apparaissent, ou sont signalés notamment par le service enquêteur, l'autorité d'habilitation ou l'officier de sécurité concerné, à la suite d'un changement de situation ou de comportement révélant un risque pour la défense nationale.

La décision portant abrogation de la décision d'habilitation (cf. IGI 1300 - annexe 12) est remise à l'intéressé, dans les mêmes formes que le refus d'habilitation. L'intéressé est informé des voies de recours contentieux ainsi que des délais qui lui sont ouverts pour

⁶¹ À l'exception d'une décision d'habilitation couvrant expressément plusieurs postes, conformément à l'article R.2311-8 du code de la défense.

⁶² Seulement lorsque la mutation dans le système SOPHIA n'est pas possible.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.6

contester la décision (cf. IM 900 - annexes 7 et 8). L'officier de sécurité s'assure que le service enquêteur est informé de cette décision.

En cas d'abrogation de sa décision d'habilitation, le titulaire signe le second volet de l'engagement de responsabilité. Il ne peut alors plus accéder à des informations et supports classifiés au risque de commettre une compromission.

Pour le personnel habilité d'une personne morale contractante, le changement d'employeur (personne morale) entraîne l'abrogation de l'habilitation.

8. Achèvement ou modification des droits associés aux fonctions

Les obligations relatives à la protection des informations et supports classifiés auxquels il a pu être donné accès perdurent au-delà du terme mis aux fonctions ou à l'habilitation de l'intéressé. Ce dernier en est informé lorsqu'il signe le second volet de l'engagement de responsabilité. Une fois signé, ce document est retourné à l'autorité d'habilitation accompagné de la décision. Il est conservé un an après la fin de validité de l'habilitation par l'autorité d'habilitation ou l'officier de sécurité de l'organisme.

Il peut apparaître nécessaire d'informer les interlocuteurs habituels ayant le besoin d'en connaître des changements intervenus chez le personnel ou au sein de l'organisme.

La chaîne de sécurité et la chaîne des ressources humaines de la formation doivent partager l'information sur les départs et arrivées des personnes habilitées. Elles s'assurent du retrait immédiat des différents droits d'accès. Elles en informent l'officier de sécurité des systèmes d'information concerné qui s'assure du retrait des droits et moyens d'accès aux systèmes d'information classifiés. Un inventaire des informations et supports classifiés dont l'intéressé a été le détenteur est établi dans les conditions énumérées au titre 5 de la présente instruction.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.7**CAS DES HABILITATIONS OTAN ET UE****Références :**

- IGI 1300 – 3.2.6 et 3.4.4
- IGI 2102/SGDSN/PSE/PSD sur la protection en France des informations classifiées de l'UE
- II 2100/SGDSN/SSD pour l'application en France du système de sécurité de l'OTAN

Points clés

- La procédure d'habilitation pour l'accès aux informations et supports classifiés OTAN et UE répond aux mêmes principes que la procédure nationale.
- Ces habilitations sont établies à partir d'un seul avis de sécurité pour un niveau d'habilitation national par l'autorité d'habilitation dont dépend le demandeur. Une habilitation délivrée par l'autorité d'habilitation pour le niveau national peut être déclinée par cette autorité pour les niveaux OTAN et UE, via une décision d'habilitation spécifique, sans refaire de demande auprès du service enquêteur.
- Le service enquêteur n'émet que des avis nationaux (*Secret, Très Secret*).
- L'habilitation nationale permet l'obtention d'une habilitation multinationale par référence, si nécessaire, tandis que la situation inverse n'est pas possible.

1. Dispositions générales

Il appartient aux autorités d'habilitation (cf. fiche 2.3) d'établir les décisions d'habilitation à connaître des informations et supports classifiés de l'Organisation du traité de l'Atlantique Nord (OTAN) et de l'Union européenne (UE). Le service enquêteur n'émet des avis de sécurité qu'au regard des niveaux d'habilitation nationaux.

Nul ne peut connaître des informations et supports classifiés de l'OTAN et des informations classifiées de l'UE (ICUE) ou de toute autre organisation internationale régie par un règlement de sécurité approuvé par la France en raison de sa qualité ou de son emploi s'il ne satisfait pas aux deux conditions suivantes :

- avoir besoin d'en connaître pour l'accomplissement de sa mission ;
- y avoir été préalablement autorisé (habilitation).

La procédure d'habilitation consiste à acquérir la garantie générale qu'une personne peut, sans risque pour la collectivité comme pour elle-même, connaître des informations et supports classifiés. Les décisions d'habilitation à accéder à des informations et supports classifiés de l'OTAN ou de l'UE sont distinctes de celles concernant la protection du secret de la défense nationale. Néanmoins, les décisions d'habilitation à accéder à des informations et supports classifiés français peuvent, en soi, à défaut d'une habilitation spécifique et sous réserve du besoin d'en connaître, donner exceptionnellement accès aux informations et supports classifiés de l'OTAN ou ICUE de niveau correspondant et des niveaux inférieurs. La situation inverse n'est pas possible.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.7

Il faut tenir compte des délais variables que peut exiger la procédure d'habilitation :

- pour l'affectation du personnel ;
- pour les prévisions de désignation du personnel à envoyer en mission, en stage, ou en liaison auprès d'organismes nationaux ou internationaux.

La procédure d'habilitation pour l'accès aux informations classifiées de l'OTAN ou de l'UE concerne le personnel qui ne possède pas l'habilitation requise au regard de la nature (UE, OTAN) ou du niveau de classification des informations et supports classifiés OTAN ou ICUE auxquels il doit accéder ou qui doit engager un renouvellement de cette habilitation.

L'habilitation est délivrée selon les procédures nationales (cf. fiches 3.1 à 3.6). Elle se concrétise par la délivrance d'une décision d'habilitation⁶³, le cas échéant accompagnée d'une mise en éveil⁶⁴ ou d'une mise en garde⁶⁵ ou d'une décision de refus⁶⁶ de cette habilitation ainsi que de mesures compensatoires, si nécessaire.

Le titulaire d'une habilitation signe l'engagement de responsabilité dans les mêmes conditions que pour l'habilitation nationale (réception et cessation d'habilitation).

2. Règles d'habilitation pour l'OTAN

Les dossiers d'habilitation, instruits par le service enquêteur, sont acheminés selon les règles définies par l'Instruction interministérielle 2100.

La décision d'accès au COSMIC TOP SECRET (CTS) ou au NATO SECRET (SO) est délivrée selon la procédure prévue pour l'accès aux informations nationales de niveau équivalent.

La décision d'habilitation au niveau NATO CONFIDENTIEL est rendue par les autorités d'habilitation du niveau NATO SECRET.

3. Règles d'habilitation pour l'UE

Les dossiers d'habilitation, instruits par le service enquêteur, sont acheminés selon les règles définies par l'Instruction interministérielle 2100. La décision d'habilitation aux niveaux TRES SECRET UE et SECRET UE est délivrée selon la procédure prévue pour l'accès aux informations nationales de niveau équivalent.

La décision d'habilitation au niveau CONFIDENTIEL UE est rendue par les autorités nationales d'habilitation du niveau Secret.

⁶³ Cf. IGI 1300 - annexe 10.

⁶⁴ Cf. IGI 1300 - annexe 9.

⁶⁵ Cf. IGI 1300 - annexe 12.

⁶⁶ Cf. IGI 1300 - annexe 14.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.7

4. Habilitations par référence

Toute décision d'habilitation émise au niveau national pour un ressortissant français peut, sous réserve du besoin d'en connaître, donner accès, de manière exceptionnelle, aux informations et supports classifiés du niveau correspondant et des niveaux inférieurs échangés dans un cadre international en application de l'accord de sécurité conclu entre les États membres de l'OTAN et des dispositions mises en place dans le cadre de l'UE.

Un certificat de sécurité peut être émis par l'autorité d'habilitation.

Attention : l'habilitation au secret de la défense nationale par référence à une habilitation OTAN ou UE n'est pas autorisée. Une demande d'habilitation nationale est nécessaire.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.8

CONTRÔLE DES RESSORTISSANTS ÉTRANGERS EN CAS D'HABILITATION OU D'ACCÈS A DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS OU CONTENANT DES INFORMATIONS *DIFFUSION RESTREINTE* OU SENSIBLES

Référence :

- IGI 1300 – 3.2.5

Points clés

- Sauf cas exceptionnel, les ressortissants étrangers peuvent être habilités au niveau *Secret* ou *Très Secret* à la condition qu'il existe un accord de sécurité, général ou spécifique, entre la France et l'État dont l'intéressé est ressortissant.
- Même habilités, les ressortissants étrangers ne peuvent avoir accès ni au *Spécial France*, ni au *Très Secret* classification spéciale.
- L'accès à des informations *Diffusion Restreinte* ou sensibles peut être autorisé aux ressortissants étrangers.

1. Habilitations des ressortissants étrangers

Les ressortissants étrangers⁶⁷, occupant une fonction nécessitant l'accès à des informations et supports classifiés, dans la limite du strict besoin d'en connaître, peuvent être habilités au niveau *Secret* ou *Très Secret* à la condition qu'il existe un accord général de sécurité, ou un accord général ou spécifique, couvrant le sujet des habilitations entre la France et l'État dont l'intéressé est ressortissant et qu'il soit déjà détenteur d'une décision nationale au niveau requis. Si un tel accord est en vigueur, deux situations peuvent se présenter :

- **le ressortissant étranger, dans le cadre d'une coopération étatique**, est muté, détaché ou en mission dans un organisme français : l'attestation d'habilitation (cf. annexe 15 IGI 1300) ou le certificat de sécurité délivré par son autorité d'habilitation d'origine peut suffire (en fonction du tableau d'équivalence de classification et des dispositions de l'accord de sécurité), à lui délivrer une décision d'habilitation lui autorisant l'accès aux informations et supports classifiés. Selon les dispositions de l'accord de sécurité, l'autorité d'habilitation française peut ainsi prendre une décision d'habilitation au regard de l'attestation de sécurité produite par l'autorité d'habilitation d'origine et, si nécessaire, émettre un certificat de sécurité ou faire mener selon les cas des compléments d'investigation auprès du service enquêteur avant de prendre une décision d'habilitation ;

⁶⁷ Conformément à l'article 22 du code civil : « la personne qui a acquis la nationalité française jouit de tous les droits et est tenue à toutes les obligations attachées à la qualité de Français, à dater du jour de cette acquisition. » Tout binational, quelle que soit l'origine de sa double nationalité, est considéré en France comme jouissant de la seule nationalité française.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.8

- **lorsque le ressortissant étranger est recruté par un organisme français**, la procédure d'habilitation est engagée par le responsable de l'organisme français concerné avec l'appui de son officier de sécurité, selon les modalités suivantes :
 - le responsable d'organisme adresse la demande d'habilitation à l'autorité d'habilitation dont il dépend, après avoir vérifié que le dossier remplit toutes les exigences ;
 - l'autorité d'habilitation, à savoir le ministre, son délégataire⁶⁸ ou l'autorité de sécurité déléguée⁶⁹, saisit le service enquêteur compétent selon les procédures habituelles ;
 - parallèlement, l'autorité d'habilitation saisit le secrétaire général de la défense et de la sécurité nationale (SGDSN), en sa qualité d'autorité nationale de sécurité⁷⁰. Cette saisine est transmise par le haut fonctionnaire correspondant de défense et de sécurité quand l'autorité d'habilitation est distincte de celui-ci ;
 - le SGDSN assure la liaison avec l'autorité nationale de sécurité étrangère soit pour obtenir l'assurance que le ressortissant étranger fait l'objet d'une habilitation ou, en cas d'absence d'habilitation, de lui demander d'habiliter ce ressortissant étranger, soit pour obtenir l'assurance qu'il n'existe aucune information défavorable sur l'intéressé de nature à constituer une vulnérabilité pour le secret de la défense nationale. Les éléments ainsi obtenus ne sont pas liants pour la délivrance de la décision d'habilitation ;
 - le SGDSN transmet les éléments reçus de son homologue étranger au HFCDs, qui les retransmet à l'autorité d'habilitation lorsque l'autorité d'habilitation est distincte de celui-ci.

Dans le cas particulier où l'autorité d'habilitation est autorité de sécurité déléguée⁷¹, et sous réserve des dispositions précisées dans la délégation du SGDSN, cette dernière saisit directement son homologue étranger pour les mêmes demandes que celles effectuées par le SGDSN et mentionnées ci-avant. L'autorité de sécurité déléguée peut, en outre, au besoin, solliciter une démarche analogue du secrétaire général de la défense et de la sécurité nationale vers l'autorité nationale de sécurité étrangère.

La décision d'habilitation n'est prise par l'autorité française d'habilitation qu'à l'issue de cette procédure.

Un ressortissant étranger habilité ne peut, en aucun cas, avoir accès à des informations et supports classifiés marqués *Spécial France*, ni à des informations et supports classifiés du niveau *Très Secret* faisant l'objet d'une classification spéciale. Son habilitation peut exclure également les informations relatives à des parties de programme ou domaines d'activité jugés sensibles au regard du pays dont le candidat à l'habilitation est ressortissant.

⁶⁸ Articles R.2311-8-1 et R.2311-8-2 du code de la défense.

⁶⁹ Cf. fiche 9.1.

⁷⁰ *Idem.*

⁷¹ Pour le ministère de la défense, la DGA est l'autorité de sécurité déléguée compétente tel que spécifié dans la note de délégation du SGDSN pour l'industrie de défense. À ce titre, elle assure le rôle d'intermédiaire entre la France et les autorités de sécurité déléguée compétentes étrangères (cf. fiche 9.1).

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.8

Afin de déterminer les conditions d'accès des ressortissants étrangers à des informations classifiées du domaine international, en particulier de ceux de l'Organisation du traité de l'Atlantique nord (OTAN) et de l'Union européenne (UE), il convient de se référer aux instructions ministérielles applicables.

Si l'habilitation concerne l'accès à des informations et supports classifiés sur un programme en coopération pour un ressortissant d'un pays tiers à cette coopération, une consultation des autres pays participants est lancée conformément aux accords de sécurité en vigueur, complétés par les stipulations précisées dans le cadre juridique de la coopération (l'instruction de sécurité programme ou les réglementations de l'OTAN, l'UE, le *European defence industry restructuring / framework* agreement – EDIR/FA, l'Organisme conjoint en matière de coopération - OCCAR).

Lorsqu'il n'existe aucun accord de sécurité entre la France et l'État dont l'intéressé est ressortissant, aucune habilitation ne peut, par principe, être délivrée par une autorité française d'habilitation. Toutefois, à titre exceptionnel, si le besoin d'en connaître est avéré et dûment motivé, le responsable d'organisme saisit le secrétaire général de la défense et de la sécurité nationale en sa qualité d'autorité nationale de sécurité qui apprécie l'opportunité de l'habilitation et définit, le cas échéant, la procédure à suivre afin que l'autorité d'habilitation puisse prendre sa décision.

2. Accès des ressortissants étrangers aux lieux contenant des informations *Diffusion Restreinte* ou sensibles

Dans les cas où l'habilitation n'est pas nécessaire, les demandes d'accueil de ressortissants étrangers dans un organisme du périmètre du ministère de la défense pouvant donner lieu à l'accès à des informations *Diffusion Restreinte* ou sensibles doivent être adressées par l'officier de sécurité de l'organisme visité au service enquêteur dans la mesure du possible au minimum deux mois avant le début du séjour. À défaut, l'officier de sécurité de l'organisme visité communique au service enquêteur, dans les meilleurs délais, les informations relatives aux visiteurs étrangers.

Ces modalités ne préjugent en rien de celles qui sont effectuées au titre de la protection du potentiel scientifique et technique de la Nation (PPSTN) en cas d'accès à une zone à régime restrictif⁷². Les modalités pratiques des séjours diffèrent suivant leur nature, la durée et le site visité.

⁷² Article R.413-5-1 du code pénal et arrêté du 03 juillet 2012 relatifs à la protection du potentiel scientifique et technique de la Nation et pour le ministère de la défense, instruction ministérielle n° 298 du 5 mars 2014 relative à la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la Nation par le ministère de la défense.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES **3.9**

ENQUÊTES ADMINISTRATIVES POUR LE RENSEIGNEMENT ET LA SÛRETÉ

Références :

La présente fiche annule et remplace la note n° 032/ARM/DPID/DR du 19 décembre 2018 relative au dispositif ministériel d'enquêtes administratives préalables à l'accès aux zones et emplois sensibles du ministère.

- Code de la défense – notamment articles L.1332-2-1, L.362-1, L.4122-11, L.4123-9-1, R.2361-1 et R.2362-1
- Code de la sécurité intérieure – notamment articles L.114-1 et R.114-1 et suivants
- Code pénal – articles 413-1 et suivants
- Code des transports - article 6224-1
- Décret n° 2014-1266 du 23 octobre 2014 relatif aux exceptions à l'application du principe « silence vaut acceptation » sur le fondement du 4° du I de l'article 21 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations ainsi qu'aux exceptions au délai de deux mois de naissance des décisions implicites sur le fondement du II de cet article (services du Premier ministre)
- Arrêté modifié du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la Nation
- IGI 1300 – 3.3.1.3, 3.5.3, 5.3.2.3

Points clés

- Le ministère de la défense distingue trois types d'enquêtes administratives pour le renseignement et la sûreté selon le niveau d'accès requis : le contrôle primaire (CP), le contrôle élémentaire (CE) et l'enquête d'habilitation.
- Une personne soumise à une enquête administrative doit en être avertie préalablement.

Le dispositif de contrôle de confiance du personnel accédant aux zones et emplois sensibles a initialement été organisé pour protéger les points d'importance vitale et préserver le secret de la défense nationale ainsi que le potentiel scientifique et technique de la Nation. Les garanties qu'il offre permettent de réduire les risques de compromission du secret, qu'elle soit volontaire (comme l'espionnage) ou accidentelle (négligence).

1. Cadre législatif et réglementaire

L'enquête administrative permet de vérifier que le comportement d'une personne physique n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.9

Le code de la sécurité intérieure (notamment son article L.114-1) permet de demander des enquêtes administratives pour le renseignement et la sûreté pour :

- autoriser l'accès aux zones protégées en raison de l'activité qui s'y exerce⁷³, notamment aux « zones militaires ou placées sous le contrôle de l'autorité militaire » ou aux zones protégées intéressant la défense nationale, aux établissements, aux installations et ouvrages d'importance vitale, etc. ;
- prendre des décisions d'autorisation, de recrutement, etc ;
- autoriser la prise de connaissance ou la détention d'informations et supports classifiés au titre du secret de la défense nationale.

Les gendarmeries spécialisées participent à la réalisation de certaines enquêtes administratives dans le cadre de protocoles établis avec les états-majors, directions et services et la DRSD.

Toute personne soumise à une enquête administrative doit en avoir été avertie au préalable⁷⁴.

Les mineurs de moins de seize ans ne peuvent pas faire l'objet d'une enquête administrative.

2. Principes généraux applicables à l'ensemble des enquêtes administratives

Le ministère de la défense distingue trois types d'enquêtes administratives pour le renseignement et la sûreté, selon le niveau de confiance requis : le contrôle primaire, le contrôle élémentaire et l'enquête d'habilitation.

Elles se différencient selon :

- le besoin qu'elles couvrent ;
- les menaces principales auxquelles elles répondent ;
- la durée de validité des avis émis.

L'enquête administrative se conclut par l'émission d'un avis, établi en fonction des informations recueillies à un instant donné, permettant d'évaluer les vulnérabilités d'une personne. Les différents avis sont donc susceptibles de révision à la demande de l'autorité décisionnelle⁷⁵ ou à l'initiative du service enquêteur.

⁷³ Pour les installations nucléaires intéressant la dissuasion ne relevant pas du ministre de la défense, au sens de l'article R.1411-9 du code de la défense, le COSSEN procède aux enquêtes administratives relatives aux personnes physiques accédant aux installations et communique les avis aux organismes demandeurs.

⁷⁴ Cf. article R. 114-6 du code de la sécurité intérieure.

⁷⁵ Autorité d'habilitation, employeur, organisme de recrutement, responsable d'emprise ou d'organisme, officier de sécurité.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES **3.9**

3. Les enquêtes administratives pour le renseignement et la sûreté

Le dispositif d'enquête administrative décrit par la présente fiche offre une garantie qui ne se substitue pas à la connaissance de l'environnement humain par l'encadrement, qui demeure une donnée essentielle de l'évaluation de la confiance.

a. Le contrôle primaire

Le contrôle primaire est une enquête administrative simple qui permet d'accéder à des lieux protégés en raison de l'activité qui s'y exerce.

Le contrôle primaire⁷⁶ donne lieu à l'émission d'un avis de sécurité (*sans objection ; vulnérabilité réduite ; vulnérabilité étendue*)⁷⁷ d'une durée de validité de trois ans au maximum, facilitant la prise de décision de l'autorité décisionnelle. Il s'applique pour l'accès aux sites du ministère de la défense, des établissements publics sous tutelle et des personnes morales liées par contrat ou convention au ministère.

Il est requis pour tous les accès dans :

- une zone protégée (ZP) ;
- un point d'importance vitale (PIV) ;
- une zone d'interdiction à la captation de données aériennes (ZICAD) ;
- une zone réservée (ZR), permanente ou temporaire.

Les autorités compétentes peuvent le requérir pour accéder à une zone militaire⁷⁸ (ZM) sur décision du responsable du site.

Le ministère de la défense peut inscrire cette disposition dans le contrat ou la convention qui le lie avec des personnes morales. Ces dernières peuvent également le mentionner dans les contrats ou conventions passés avec leurs sous-traitants et sous-contractants.

Les personnes suivantes peuvent faire l'objet d'un CP lorsqu'elles accèdent aux lieux cités supra :

- personnel permanent et stagiaire du ministère de la défense, des établissements publics sous tutelle et des personnes morales liées par contrat ou convention au ministère de la défense ;
- prestataires (personnel employé par des personnes morales de droit privé liées par contrat sensible ou classifié au ministère de la défense) ;

⁷⁶ Demande de type CPR sur SOPHIA.

⁷⁷ Le formulaire de CP du système SOPHIA comporte seulement deux cases : sans objection (SO) ou autre que sans objection (AQSO) : les 3 niveaux sont mentionnés en commentaire.

⁷⁸ L'article 413-5 du code pénal, auquel fait référence l'article R.2361-1 du code de la défense relatif aux zones militaires mentionne « un terrain, un port, une construction ou un engin ou appareil quelconque affecté à l'autorité militaire ou placé sous son contrôle ». Il est à noter qu'un terrain privé occupé par le ministère de la défense pour ses services par le biais d'une convention de location peut être qualifié de zone militaire au sens du code de la défense et du code pénal.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.9

- prestataires liés à l'exécution d'un marché dans le cadre d'une demande de dérogation d'une ZICAD ;
- intervenants ou accédants sous convention⁷⁹ avec le ministère de la défense.

Les personnes, accédant sans contrôle primaire, sont obligatoirement accompagnées et leurs déplacements sont encadrés. Cette disposition s'applique en particulier aux visiteurs et aux personnes convoquées dans le cadre des Journées Défense-Citoyenneté.

Dans le cas d'un accès à une emprise incluse dans un site rassemblant plusieurs emprises, l'officier de sécurité du site formule une demande de contrôle primaire. En cas d'avis autre que sans objection, il en informe l'officier de sécurité de l'emprise accueillante et statue avec lui sur les suites à donner et les mesures à prendre.

Dans le cas d'une personne morale soumissionnant à un contrat sensible, le contrôle primaire du représentant légal de cette personne morale peut être sollicité par l'autorité contractante parmi les documents constitutifs de l'enquête administrative décrite à la fiche 4.10 de la présente instruction.

Le **contrôle primaire intermédiaire**⁸⁰ est un contrôle régulier des personnes en raison du type d'emprises auxquelles elles accèdent, des emplois qu'elles occupent ou des informations et supports sensibles ou classifiés auxquelles elles ont accès.

Il donne lieu à l'émission d'un avis de sécurité (*sans objection ; vulnérabilité réduite ; vulnérabilité étendue*).

Il est réalisé à un rythme adapté aux employeurs en fonction des vulnérabilités et de la sensibilité des fonctions occupées, après accord de la DRSD.

Le contrôle primaire et le contrôle primaire intermédiaire sont également confiés aux gendarmeries spécialisées dans le cadre d'un protocole réalisé en concertation avec les états-majors, directions et services et la DRSD.

b. Le contrôle élémentaire

Le contrôle élémentaire (CE) est une enquête administrative sollicitée par l'employeur, l'organisme de recrutement, le commandant de formation administrative, le chef d'établissement (CFA/CE) ou par l'intermédiaire de l'officier de sécurité. Il est destiné à s'assurer du degré de confiance d'une personne en vue :

- d'être recruté comme militaire ou agent civil (fonctionnaire ou contractuel) du ministère de la défense⁸¹ ;
- d'exercer un emploi dans une des fonctions décrites en annexe 1⁸² ;
- d'accéder à une zone à régime restrictif (ZRR)⁸³.

⁷⁹ Ex : adhérents aux clubs sportifs et artistiques de la défense.

⁸⁰ Demande de type CPR sur SOPHIA.

⁸¹ Demande de type CER sur SOPHIA. Le contrôle élémentaire est obligatoire pour le recrutement des militaires et des agents civils affectés à des emplois pérennes. Une directive ministérielle fixe les modalités de réalisation de ces contrôles pour les agents civils du ministère.

⁸² Demande sur SOPHIA de type CES (ou CNV pour le cas particulier des convoyeurs d'informations et supports classifiés).

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES **3.9**

Les conclusions techniques de cette enquête, effectuée exclusivement par le service enquêteur, donnent lieu à l'émission d'un avis de sécurité⁸³ (*sans objection/ restrictif/ défavorable*) adressé à l'autorité décisionnelle.

La durée de validité de cet avis n'excède pas trois ans à l'exception des accès à une zone à régime restrictif, dont la durée de validité maximum est de cinq ans.

c. L'enquête d'habilitation

L'enquête d'habilitation vise à assurer l'autorité d'habilitation du degré de confiance pouvant être accordé à une personne ayant besoin d'accéder ou accédant déjà à des informations et supports classifiés.

Le service enquêteur émet un avis de sécurité (*sans objection, restrictif ou défavorable*), accompagné pour les avis autres que sans objection d'une fiche confidentielle, qui permet à l'autorité d'habilitation d'accorder ou de refuser une décision d'habilitation à connaître des informations couvertes par le secret de la défense nationale.

La durée maximum de cet avis est fonction du niveau de l'habilitation demandée. Elle ne peut excéder :

- **sept ans** pour le niveau *Secret* ;
- **cinq ans** pour le niveau *Très Secret*.

4. Extension de la portée des avis de sécurité

Un avis de sécurité peut être valable au titre de plusieurs enquêtes administratives (contrôle primaire, contrôle élémentaire et habilitation) s'il remplit les conditions suivantes :

- il est sans objection ;
- en cas d'enquêtes administratives multiples, l'avis le plus récent doit être pris en compte ;
- il a été émis moins de trois ans auparavant ;
- à son expiration ou lors d'un changement de situation justifiant sa révision, une nouvelle enquête administrative doit être réalisée.

Les avis de sécurité délivrés à des ressortissants étrangers ne peuvent pas être valables au titre de plusieurs enquêtes administratives.

En outre, les avis de sécurité délivrés dans le cadre d'une demande d'autorisation d'accès en zone à régime restrictif ne peuvent être étendus à d'autres enquêtes

⁸³ Demande de type AZR sur SOPHIA. Cette disposition répond à une politique de sécurité particulière encadrée par une instruction ministérielle dédiée (IM 298), destinée aux organismes du ministère, établissements publics sous tutelle et personnes morales liées par contrat ou convention.

⁸⁴ Pour l'accès en zone à régime restrictif.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES 3.9

administratives pour le renseignement et la sûreté que pour une durée maximale de trois ans.

a. L'extension de portée verticale

Une personne physique ayant fait l'objet d'un avis de sécurité sans objection datant de moins de 3 ans émis dans le cadre d'une enquête d'habilitation ou d'un contrôle élémentaire est réputée détenir un avis tacite sans objection à un contrôle primaire. Il n'est donc pas nécessaire de réaliser une nouvelle enquête, ni d'émettre formellement un nouvel avis durant cette période.

b. L'extension de portée horizontale

Une personne physique ayant fait l'objet d'un contrôle primaire datant de moins de trois ans est réputée détenir un avis tacite sans objection à tout autre contrôle primaire. Il n'est donc pas nécessaire de réaliser une nouvelle enquête, ni d'émettre formellement un nouvel avis durant cette période.

5. Révision des avis et décisions

Le responsable d'organisme doit s'assurer que le comportement d'une personne autorisée à tenir un poste à l'issue d'une enquête administrative est toujours compatible avec les exigences de ce poste⁸⁵. À cet effet, il peut saisir le service enquêteur et demander la réalisation d'une nouvelle enquête administrative.

Au sein des services du ministère, lorsque cette nouvelle enquête administrative fait apparaître que le comportement d'un fonctionnaire est effectivement devenu incompatible avec l'exercice de ses fonctions, le ministère procède à son affectation ou à sa mutation dans l'intérêt du service dans un emploi comportant l'exercice d'autres fonctions. En cas d'impossibilité de mettre en œuvre une telle mesure ou lorsque le comportement du fonctionnaire est incompatible avec l'exercice de toute autre fonction eu égard à la menace grave qu'il fait peser sur la sécurité publique, il est procédé, après une procédure contradictoire à sa radiation des cadres.

En outre, à l'exception du changement d'affectation, cette procédure inclut l'avis de la commission, prévue aux dispositions du IV de l'article L.114-1 et aux articles R.114-6-1 du code de la sécurité intérieure.

Lorsque le résultat de l'enquête fait apparaître que le comportement **d'un agent contractuel de droit public** est devenu incompatible avec l'exercice de ses fonctions, son employeur lui propose un emploi comportant l'exercice d'autres fonctions et correspondant à ses qualifications. En cas d'impossibilité de mettre en œuvre une telle mesure, en cas de refus de l'agent ou lorsque son comportement est incompatible avec l'exercice de toute autre fonction eu égard à la menace grave qu'il fait peser sur la

⁸⁵ Il de l'article L.114-1 du code de la sécurité intérieure.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES **3.9**

sécurité publique, il est procédé, après mise en œuvre d'une procédure contradictoire, à son licenciement.

Pour les **militaires**, lorsque le résultat d'une enquête administrative fait apparaître que le comportement d'un militaire est devenu incompatible avec l'exercice de ses fonctions eu égard à la menace grave qu'il fait peser sur la sécurité publique, il est procédé, après mise en œuvre d'une procédure contradictoire, à sa radiation des cadres ou à la résiliation de son contrat.

Ces mesures interviennent après avis d'un conseil dont la composition et le fonctionnement sont fixés par décret en Conseil d'État.

Ces décisions peuvent être contestées devant le juge administratif dans un délai de quinze jours à compter de leur notification et faire l'objet d'un appel et d'un pourvoi en cassation dans le même délai. Les juridictions saisies au fond statuent dans un délai de deux mois. En cas de recours, la décision contestée ne peut prendre effet tant qu'il n'a pas été statué en dernier ressort sur ce litige.

L'employeur peut décider, à titre conservatoire, et pendant la durée strictement nécessaire à la mise en œuvre des suites données au résultat de l'enquête, d'écarter sans délai du service le militaire, fonctionnaire ou l'agent contractuel de droit public, avec maintien de son traitement ou de sa solde, de l'indemnité de résidence, du supplément familial de traitement et des prestations familiales obligatoires⁸⁶.

Si le résultat de l'enquête administrative fait apparaître que le comportement d'un salarié occupant un emploi participant à l'exercice de missions de souveraineté de l'État ou relevant du domaine de la sécurité ou de la défense est devenu incompatible avec l'exercice de ses fonctions et a entraîné l'abrogation de son habilitation, la personne morale qui l'emploie peut procéder à son affectation ou à sa mutation dans l'intérêt du service dans un emploi comportant l'exercice d'autres fonctions ne nécessitant pas une habilitation. En cas d'impossibilité de mettre en œuvre une telle mesure⁸⁷ ou lorsque le comportement du salarié est incompatible avec l'exercice de toute autre fonction, son licenciement peut être prononcé. Ces dispositions doivent avoir été préalablement insérées dans une clause du contrat de travail dudit salarié pour être effectives⁸⁸.

6. Autres enquêtes administratives

Ces enquêtes administratives sont soumises aux principes précisés au point 2. du présent titre.

a. Le contrôle d'accès à la donnée de militaire⁸⁹

⁸⁶ Voir l'articles L.114-1 du code de la sécurité intérieure et L.4139-15-1 du code de la défense.

⁸⁷ Exemple d'une entreprise dans laquelle tous les postes requièrent une habilitation.

⁸⁸ Clause de protection du secret prévue par l'IGI 1300 annexe 17, point 4.

⁸⁹ Article L.4123-9-1 du code de la défense.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES **3.9**

Le contrôle d'accès à la donnée de militaire (CAD) s'applique dans les conditions définies dans la fiche « Protection des données à caractère personnel comportant la mention de la qualité de militaire » (3.11). Il vise à protéger les militaires et prévenir les vulnérabilités associées à une potentielle divulgation de données personnelles ou professionnelles.

Il donne lieu à une enquête administrative qui a pour finalité d'identifier si les personnes qui accèdent aux données à caractère personnel de militaires constituent une menace pour leur sécurité. Le service enquêteur rend un avis (*sans objection, défavorable*).

Ce n'est que dans l'hypothèse où le ministre compétent considère, sur le fondement de l'enquête administrative, que cette menace est caractérisée, qu'il en informe sans délai le responsable du traitement qui est alors tenu de refuser à ces personnes l'accès aux données à caractère personnel de militaires y figurant.

b. Le contrôle des savoir-faire sensibles

En application des articles L.4122-11 et L.4122-13 du code de la défense, le militaire exerçant des fonctions présentant une sensibilité particulière ou requérant des compétences techniques spécialisées ou l'agent civil de l'État et de ses établissements publics participant au développement de savoir-faire nécessaires à la préparation et à la conduite des opérations militaires, qui souhaite exercer une activité dont il retire un avantage personnel ou une rémunération dans le domaine de la défense ou de la sécurité au bénéfice, direct ou indirect, d'un État étranger, d'une collectivité territoriale étrangère ou d'une personne morale ou d'une organisation ayant son siège en dehors du territoire national ou sous contrôle étranger, est tenu d'en faire la déclaration au ministre de la défense.

Cette obligation de déclaration vaut pour une durée de dix ans suivant la cessation de ses fonctions.

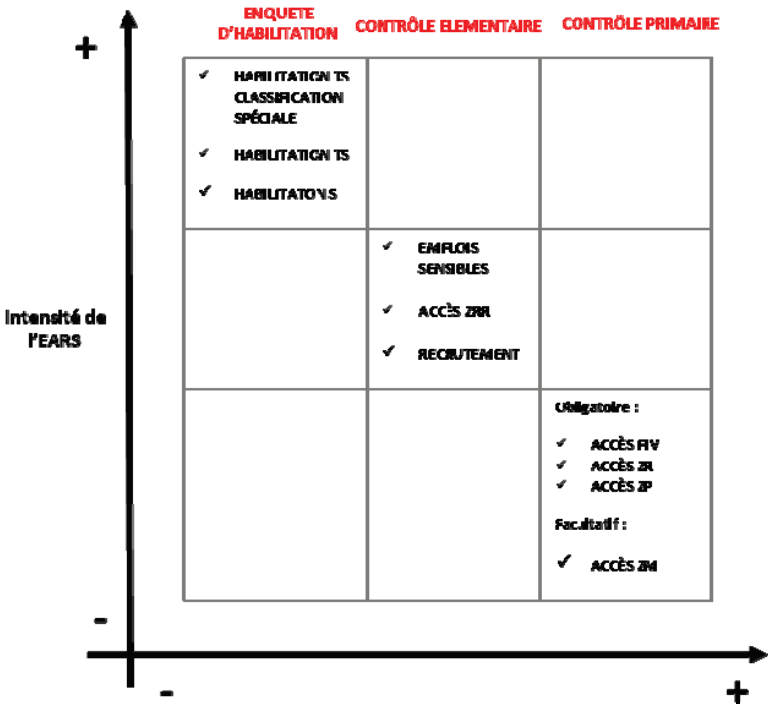
Les éléments recueillis sont communiqués au ministre de la défense qui peut émettre une décision d'opposition à l'exercice de l'activité envisagée par le demandeur.

Afin de pouvoir prendre sa décision en connaissance de cause, une enquête administrative est réalisée⁹⁰.

⁹⁰ Cf. p) du 1^o de l'article R.114-2 du code de la sécurité intérieure.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES
PHYSIQUES

3.9



**TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES
PHYSIQUES****3.10****OBLIGATION DE RÉSERVE, DISCRÉTION PROFESSIONNELLE ET
SECRET PROFESSIONNEL POUR LES AGENTS DU MINISTÈRE DE LA
DÉFENSE****Références :**

- Code de la défense (livre premier portant statut général des militaires) – articles L.4121-2 et L.4122-4
- Code général de la fonction publique – articles L.121-6, L.121-7 et L.135-1 à L.135-5
- Code pénal – article 226-13 (atteinte au secret professionnel) et articles 413-9 à 413-14 (atteintes au secret de la défense nationale)
- Code de procédure pénale – article 40
- Décret n° 2015-386 du 3 avril 2015 fixant le statut des fonctionnaires de la direction générale de la sécurité extérieure
- Décret n° 2021-246 du 3 mars 2021 relatif aux dispositions générales applicables aux agents contractuels de la direction générale de la sécurité extérieure
- Décret n° 2023-1039 du 15 novembre 2023 modifiant les dispositions générales applicables aux fonctionnaires et aux agents contractuels de la direction générale de la sécurité extérieure
- IGI 1300 – 3.4.3

Points clés

- Faire état, directement ou indirectement, de sa qualité de personnel du ministère de la défense engage l'image de l'institution. Il convient donc de respecter le devoir de réserve et les règles de discrétion et de secret professionnel.
- Toute information diffusée alors qu'elle n'est pas destinée au public peut présenter des risques pour la sécurité du personnel, la sécurité des opérations et peut porter atteinte à l'image du ministère.

Au-delà du respect du secret de la défense nationale, les agents du ministère, militaires comme civils, sont soumis à une obligation de réserve, au devoir de discrétion et, le cas échéant, au respect du secret professionnel. Ainsi, la communication d'informations d'origine professionnelle s'inscrit dans un cadre juridique visant à protéger ces informations afin, notamment, de ne pas compromettre les opérations en cours ou à venir et, plus largement, de ne pas porter atteinte à l'image de l'institution par dénigrement ou par brouillage de la communication officielle.

1. Champ d'application

Ces dispositions s'appliquent quel que soit le mode d'expression choisi.

Sont concernés les militaires d'active ou de réserve et les agents civils du ministère, ouvriers, fonctionnaires ou contractuels.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES **3.10**

2. Obligations

a. Obligation de réserve

Le personnel du ministère de la défense doit faire preuve de réserve et de mesure dans l'expression écrite et orale de ses opinions personnelles. Il s'interdit, afin de préserver le bon fonctionnement du service, tout propos de nature à porter préjudice à la considération et à la confiance dont l'administration et ses autorités doivent bénéficier.

L'obligation de réserve s'applique pendant et en dehors des heures de service. Il en est de même pour les agents suspendus de leurs fonctions ou en disponibilité.

b. Discretion professionnelle

La discretion professionnelle est requise au sein du ministère de la défense afin d'éviter la divulgation d'informations relatives à l'activité ou au fonctionnement de l'administration ou au déroulement des opérations militaires. Ce devoir de discretion concerne les documents, informations ou faits qui n'ont pas vocation à être communiqués au public.

Cette obligation s'applique hors de l'environnement professionnel mais également à l'égard des personnes qui n'ont pas le besoin d'en connaître. Elle peut être levée par décision de l'autorité hiérarchique.

c. Secret professionnel

La mention *Diffusion Restreinte* n'est pas un niveau de classification mais une mention de protection et n'a ainsi pas pour effet de conférer la protection pénale propre au secret de la défense nationale. Pour autant, la divulgation d'informations et supports portant la mention *Diffusion Restreinte* à des personnes physiques ou morales n'ayant pas le besoin d'en connaître est susceptible d'exposer son auteur à des sanctions disciplinaires, administratives et éventuellement pénales, notamment au titre de la violation du secret professionnel.

La violation du secret professionnel est punie d'un an d'emprisonnement et de 15 000€ d'amende.

3. Cas particulier des lanceurs d'alerte et de l'article 40 du code de procédure pénale

Le lanceur d'alerte est une personne physique qui révèle ou signale, sans contrepartie financière directe et de bonne foi, des informations sur :

- un crime (vol aggravé, viol, faux en écriture publique, etc.) ou un délit (corruption, prise illégale d'intérêts, trafic d'influence, usage illégal de fonds publics, harcèlement moral ou sexuel, discrimination, etc.) ;
- la violation grave et manifeste d'un engagement international, d'une loi ou d'un règlement ;
- toute menace ou préjudice grave pour l'intérêt général.

**TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES
PHYSIQUES****3.10**

Il doit avoir eu personnellement connaissance des faits constitutifs de l'alerte.

Le lanceur d'alerte bénéficie de garanties accordées par la loi. La confidentialité de son identité doit être respectée et il ne peut être sanctionné ou faire l'objet d'une mesure discriminatoire pour avoir signalé une alerte. Cette dernière protection vaut pour les militaires. Ils peuvent saisir une autorité externe de recueil des signalements qui respectera les garanties prévues par la loi. Pour les sujets du périmètre défense, ces autorités externes sont le Contrôle Général des Armées (CGA) et le collège des Inspecteurs généraux des Armées (IGA). Les faits couverts par le secret de la défense nationale sont exclus du régime de l'alerte tel que défini par la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (article 6). Tout signalement abusif peut entraîner des conséquences sur le plan pénal ou disciplinaire.

Aux termes de l'article L.861-3 du code de sécurité intérieure, les agents des services de renseignement qui ont connaissance, dans l'exercice de leurs fonctions, de faits susceptibles de constituer une violation manifeste du livre VIII du code de la sécurité intérieure peuvent saisir la Commission nationale de contrôle des techniques de renseignement (CNCTR), y compris pour des faits couverts par le secret de la défense nationale.

Indépendamment du régime du lanceur d'alerte, tout agent civil ou militaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu, en vertu de l'article 40 du code de procédure pénale, d'en donner avis sans délai au procureur de la République. Il s'agit d'une obligation mais qui vise les seuls crimes et délits dont l'intéressé a eu connaissance dans l'exercice de ses fonctions, si ces faits lui paraissent suffisamment établis.

**TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES
PHYSIQUES****3.11****PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL
COMPORTANT LA MENTION DE LA QUALITÉ DE MILITAIRE****Références :**

- Règlement (UE)2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE
- Code de la défense – articles L.4123-9-1, R.4123-45 et suivants (personnel militaire)
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles

Points clés

- Pour des raisons de sécurité, le traitement de données à caractère personnel qui permet de révéler la qualité de militaire d'une personne est par principe interdit.
- Par exception, ce traitement peut être autorisé uniquement lorsqu'il est strictement nécessaire à l'une des finalités du traitement. Dans ce cas, il doit faire l'objet d'une attention particulière et d'une déclaration auprès de la direction du renseignement et de la sécurité de la défense.

1. Définition

Une donnée est qualifiée de donnée à caractère personnel de militaire (DCPM) dès lors qu'elle associe :

- un ou plusieurs éléments permettant d'identifier une personne (ex. nom, prénom, photographie) ;
- un ou plusieurs éléments révélant sa qualité de militaire (ex. indication du grade, port de l'uniforme sur une photographie).

Le **responsable de traitement** est une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Les systèmes numériques traitant de données à caractère personnel des agents du ministère de la défense se regroupent en quatre catégories :

- les systèmes numériques internes au ministère de la défense ;
- les systèmes numériques d'organismes sous tutelle, y compris les établissements publics ;
- les systèmes numériques dépendants de prestataires extérieurs ;
- les systèmes numériques d'organismes externes sans lien contractuel ni institutionnel avec le ministère de la défense (entreprises, associations, etc.).

À cette liste s'ajoutent les systèmes numériques internes des entités contractantes avec le ministère, qui traitent des DCPM.

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES**3.11****Principe : interdiction de traiter des données à caractère personnel de militaire**

L'utilisation de ces données est susceptible de porter atteinte à la sécurité de la personne concernée et de son cercle familial et de nuire aux intérêts de l'État, de permettre d'exercer des menaces ciblées sur les opérations et les activités du ministère, de ses entités sous tutelle ou cocontractantes.

En conséquence, le traitement des DCPM est par principe interdit.

→ Si le responsable de traitement traite de données professionnelles, il doit par exemple privilégier la mention d'agent public à la place de celle de militaire.

Exception : si les données à caractère personnel de militaire sont strictement nécessaires à la poursuite d'une finalité de traitement.

Le responsable de traitement doit s'interroger sur la nécessité de traiter des données à caractère personnel de militaire. Ce traitement n'est autorisé que si aucune autre procédure ne peut être mise en œuvre.

Si tel est le cas, le responsable de traitement informe sans délai la direction du renseignement et de la sécurité de la défense⁹¹. Il lui précise les principales caractéristiques du traitement, en particulier ses finalités, les catégories de données collectées, les éventuels destinataires de ces données, les mesures techniques et organisationnelles ainsi que le nombre de personnes accédant aux données à caractère personnel de militaires⁹².

La DRSD, service enquêteur du ministère de la défense, peut réaliser une enquête administrative de sécurité sur les personnes accédant aux données à caractère personnel de militaire aux seules fins d'identifier si elles constituent une menace pour la sécurité des militaires concernés.

Si le ministre de la défense considère, sur le fondement de l'enquête administrative, que cette menace est caractérisée, il en informe sans délai le responsable de traitement qui est alors tenu de refuser à ces personnes l'accès aux données à caractère personnel de militaire y figurant.

Ne pas respecter cette obligation de déclaration ou donner l'accès à ces données à une personne pour laquelle le ministre a émis un avis défavorable sont des faits constitutifs des délits prévus à l'article L.4123-9-1 du code de la défense.

2. Mesures de sécurité

Les dispositions du 2 de l'article 25 du RGPD ainsi que du 6° de l'article 4 de la loi dite « informatique et libertés » imposent que toute donnée à caractère personnel soit traitée de façon à garantir une sécurité appropriée, à l'aide de mesures techniques et organisationnelles. La particularité des données à caractère personnel de militaire

⁹¹ À l'adresse suivante : drsd-dcpm-declaration.accueil.fct@intradef.gouv.fr.

⁹² Article R.4123-46 du code de la défense.

**TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES
PHYSIQUES****3.11**

impose, en conséquence, un niveau de sécurité renforcé respectant, notamment, les points visés au titre 6 de la présente instruction ministérielle, relatif à la sécurité des systèmes d'information pour les personnes morales de droit privé.

En cas de tentative d'attaque ou d'incident pouvant avoir mené à une divulgation de DCPM, le responsable de traitement informe sans délai :

- son délégué à la protection des données ;
- sa chaîne de lutte informatique et défensive le cas échéant ;
- la DRSD.

Dans le cas où le responsable de traitement ne procède pas, y compris par négligence, à la notification à la DRSD, il peut voir sa responsabilité pénale engagée et encourir, conformément au 3^o du IV de l'article L.4123-9-1 du code de la défense, la peine de trois ans d'emprisonnement et de 300 000 euros d'amende.

Des dispositifs de protection de ces données à caractère personnel de militaire permettent de limiter la diffusion de l'identité du personnel travaillant au sein du ministère de la défense.

En raison de la nature sensible des postes que peut occuper le personnel des organismes contractants (ex. industriels d'armement), des dispositifs de protection doivent également être appliqués.

a. Rôle des états-majors, directions et services

Les états-majors, directions et services sont chargés de mener les actions de sécurité vis-à-vis des trois premières catégories de systèmes numériques énoncées au 1. Chaque entité a pour tâche de recenser et catégoriser ses détenteurs de données et de prendre contact avec les entités extérieures susceptibles de traiter ces données à caractère personnel de militaire.

Au sein du ministère, les mesures de protection doivent être adaptées au niveau de la menace. Elles se traduisent par une homologation permanente de ces systèmes numériques et, en cas de risque identifié, par des mesures immédiates de renforcement de la sécurité laissées à l'appréciation du responsable de traitement en lien avec l'autorité qualifiée en sécurité des systèmes d'information (AQSSI). De manière générale, les fichiers réalisés pour le compte de l'État sont soumis aux exigences de la politique de sécurité des systèmes d'information (PSSI-M).

Le ministère de la défense s'assure également de la sensibilisation aux menaces de son personnel et des organismes sous tutelle et de la mise en place des mesures appropriées. Il en est de même pour les prestataires extérieurs, qui sont, de surcroît, soumis à des obligations contractuelles adaptées au traitement de ces données à caractère personnel de militaire.

Concernant les systèmes numériques d'organismes externes sans lien contractuel ni institutionnel avec le ministère, les états-majors, directions et services sont invités à contribuer à la sensibilisation des entités identifiées et à signaler au Commissariat au Numérique de Défense (CND) les entités dont les faiblesses constatées en matière de

TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES PHYSIQUES

3.11

sécurité des données à caractère personnel de militaire pourraient nécessiter un dialogue particulier.

b. Rôle du responsable d'organisme contractant

Le responsable d'organisme applique, via son autorité qualifiée en sécurité des systèmes d'information, le même type de mesures qu'énoncées précédemment pour assurer la protection des données à caractère personnel de militaire de son personnel, à savoir :

- recensement et catégorisation de ses détenteurs de données ;
- homologation permanente de ses systèmes numériques ;
- gestion des fichiers soumis à la PSSI de l'entité ;
- sensibilisation de son personnel aux menaces.

c. Rôle du responsable de traitement

Les responsables de traitement sont soumis à quatre principes de sécurité :

1. Ne collecter ou conserver que les données pertinentes : le responsable de traitement s'assure que seules sont collectées et conservées les données pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
2. Maîtriser les exports de données : les transferts de données vers un tiers (sous-traitant par exemple) sont réduits au strict minimum ou filtrés (suppression d'une partie des informations) afin de ne pas divulguer de données à caractère personnel de militaire. Les obligations afférentes en matière de sécurité des données doivent être mentionnées dans les conventions ou contrats (nature des traitements, durée de conservation, transferts ultérieurs, etc.).
Les exports de données peuvent aussi concerner la mise en ligne, par exemple au travers d'un site web ou l'utilisation de technologies de type informatique en nuage (*cloud computing*). Un niveau de protection technique adéquat des données doit être assuré.
3. Mettre en place des mécanismes de contrôle d'accès et d'imputation : les SI manipulant des données à caractère personnel de militaire doivent permettre de contrôler et d'imputer l'accès aux données pour ne l'accorder qu'aux personnes autorisées et dûment identifiées.
4. Gérer les incidents relatifs aux données à caractère personnel de militaire : le responsable de traitement informe sans délai en cas de tentative d'attaque ou d'incident pouvant avoir mené à une divulgation de données à caractère personnel la chaîne de lutte informatique défensive (LID), la DRSD et le délégué à la protection des données⁹³ (pour le ministère : daj.delegue.fct@intradef.gouv.fr).

⁹³ Toute violation de sécurité doit donner lieu à une information du délégué à la protection des données (DPD) en application des articles 33 et 34 du règlement européen sur la protection des données personnelles et des procédures du règlement européen sur la protection des données personnelles en place au sein du ministère dans un délai de 72h (cf. instruction ARM/SGA/DAJ/D2P/DPSP du 31 janvier 2020 relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense).

**TITRE 3 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES
PHYSIQUES**

3.11**d. Protection juridique du personnel du ministère de la défense en matière de
protection des données personnelles et de respect de l'anonymat**

Plus largement, la protection juridique du personnel du ministère de la défense (civils et militaires) en matière de protection des données (traitées par le ministère de la défense ou par d'autres organismes) et d'anonymat est définie dans le tableau ci-après.

TITRE 3 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
PHYSIQUES

3.11

	Dispositions	Tout ministère		Services spécialisés		Entités contractantes	
		Personnel civil (PC)	Personnel militaire (PM)	Services de renseignement (PM / PC)	Forces spéciales (PM)	Personnel civil (PC)	Personnel militaire (PM)
Protection des données	Règlement européen sur la protection des données (RGPD) et loi 78-17 du 06/01/1978 modifiée dite "loi informatique et liberté" -> fichiers de droit commun	X	X	X	X	X	X
		X	X	X	X	X	X
		X	X	X	X	X	X
		X	X	X	X	NC	NC
	Loi 78-17 du 06/01/1978 modifiée dite "loi informatique et liberté", article 31 -> fichiers de souveraineté	NC	NC	NC	NC	NC	NC
		selon les dispositions de l'acte réglementaire portant création du traitement de données concerné				NC	NC
	Article L. 4123-9-1 du code de la défense (introduit par l'article 117 de la loi n° 2016-731 du 03/06/2016) Articles R. 4123-45 et s. du code de la défense Loi n° 2018-493 du 20 juin 2018 relative à la protection des données (l de l'article 16)	NC	NC	NC	NC	NC	X
		NC	NC	NC	NC	NC	X
	Article 226-17-1 du code pénal	(excepté pour les fichiers de souveraineté)		X		X	X
	Article 226-16 du code pénal	X	X	X	X	X	X
Protection de l'anonymat	Loi du 29/07/1981 sur la presse Arrêté du 7 avril 2011 relatif à l'anonymat	X	X	X	X	X	X
	Article 861-1 du code de la sécurité intérieure - services spécialisés de renseignement (L.871-2 CSJ) - autres services autorisés à recourir aux techniques de renseignement (L.871-4 CSJ)	X	X	X	X	NC	NC
	Article 413-13 du code pénal	X	X	X	X	X	X
	Article 413-14 du code pénal Arrêté du 20 octobre 2016 fixant la liste des unités spéciales concernées	NC	X	X	X	X	X

TITRE 4 : MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

INTRODUCTION : PRINCIPES GÉNÉRAUX DE LA PROTECTION DU SECRET ET DE SÉCURITÉ NUMÉRIQUE DANS LES CONTRATS

Référence :

- IGI 1300 – 4

Points clés

- La réglementation relative à la protection du secret encadre les contrats impliquant l'accès ou la détention d'informations et supports classifiés ainsi que les contrats sensibles. Il est néanmoins possible d'introduire des mesures de protection dans n'importe quel type de contrat.
- Le besoin de protection des informations et supports classifiés et des informations sensibles ou *Diffusion Restreinte* est exprimé par le prescripteur technique.
- La mise en œuvre des mesures de protection comprises dans le contrat incombe à la personne morale.
- Seuls les contrats impliquant l'accès ou la détention d'informations et supports classifiés nécessitent l'habilitation de la personne morale.
- L'habilitation éventuelle d'un administrateur de système numérique de niveau maximal *Diffusion Restreinte* n'est pas conditionnée par l'habilitation de la personne morale à laquelle il appartient.
- L'habilitation de la personne morale doit être obtenue avant la signature du contrat.
- À l'exception de son représentant légal et en dehors des phases précontractuelles, l'habilitation de la personne morale est le préalable indispensable à l'habilitation du personnel de la société, sauf lorsque celle-ci possède la qualité d'opérateur d'importance vitale.

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

Les principes évoqués dans la présente fiche s'appliquent à toute convention et tout contrat de la commande publique (marché public ou concession), à tout contrat de sous-traitance ou de sous-contractance, quel que soit leur régime juridique ou leur dénomination, pour l'exécution desquels doivent être prises des mesures de protection du secret de la défense nationale et de sécurité numérique.

La sensibilité des informations dans les contrats passés entre le ministère de la défense et les personnes morales ainsi que leurs sous-traitants et sous-contractants notamment exige la prise en compte rigoureuse des besoins de protection dans les contrats dès l'engagement de la consultation ou dès l'envoi à la publication de l'avis d'appel à la concurrence. Le rôle du prescripteur technique est à ce titre essentiel. Il doit préciser le besoin de protection du secret de la défense nationale et des systèmes numériques contribuant à la réalisation du contrat dès le début de la procédure précontractuelle. Ce besoin de protection peut inclure les informations et supports *Diffusion Restreinte* et sensibles de même que certains systèmes numériques. Il doit également préciser le devenir des informations et données classifiées, *Diffusion Restreinte* ou sensibles ainsi que les supports associés à la fin de l'exécution du contrat (destruction ou restitution à l'autorité contractante par exemple).

La mise en œuvre de ces mesures incombe aux représentants légaux des personnes morales. Les personnes morales titulaires des contrats se doivent en effet de mettre en œuvre les prescriptions réglementaires et contractuelles pour assurer la sécurité des informations et supports classifiés et des systèmes numériques. Cette responsabilité vaut également vis-à-vis des sous-traitants et sous-contractants de tout rang.

À toutes les phases d'une procédure d'achat, il appartient également au représentant légal de la personne morale de veiller à la stricte et constante application des dispositions législatives et réglementaires applicables au site militaire de la part de son personnel, comme de ses sous-traitants et sous-contractants, notamment l'interdiction, dans une zone fixée par l'autorité militaire et faisant l'objet d'une signalisation particulière, d'effectuer des dessins, levés ou enregistrements d'images, de sons ou de signaux sans l'autorisation de cette autorité.

1. Expression du besoin de protection

Au regard de la protection des informations existent plusieurs types de contrats :

- les contrats qui nécessitent l'habilitation préalable du contractant :
 - o contrats impliquant l'accès à des informations et supports classifiés sans détention ;
 - o contrats impliquant l'accès et la détention d'informations et supports classifiés ;
 - o contrats impliquant la détention d'informations et supports classifiés sur un système numérique.
- les contrats sensibles.

Au-delà de ces types de contrats encadrés par la réglementation relative à la protection du secret de la défense nationale et décrits dans la présente instruction, des mesures

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

ponctuelles de protection des informations sensibles ou des mesures de défense-sécurité peuvent être intégrées dans n'importe quel type de contrat⁹⁴.

Pour toute procédure de passation devant aboutir à un contrat impliquant l'accès ou la détention d'informations et supports classifiés (cf. fiche 4.5 et suivantes), à la mise en œuvre des systèmes numérique soumis à une réglementation ou des normes de sécurité ou à un contrat sensible (cf. fiche 4.3), le prescripteur technique, avec le concours de son officier de sécurité, doit préciser lors de la demande d'achat le besoin de protection concernant la préparation et l'exécution du contrat.

L'expression de ce besoin fait l'objet d'une fiche de besoin de protection du secret⁹⁵, rédigée sous la responsabilité du prescripteur technique avec le concours de l'officier de sécurité et de l'officier de sécurité des systèmes d'information et, le cas échéant, de l'autorité contractante, qui doit impérativement être jointe à la demande d'achat.

2. Habilitation de la personne morale

L'habilitation d'une personne morale correspond au besoin de l'administration d'apprécier les garanties présentées avant d'attribuer un contrat de la commande publique avec accès ou détention d'informations et supports classifiés.

La décision d'habilitation permet :

- à une autorité contractante d'attribuer des contrats de la commande publique comportant l'accès ou la détention d'informations et supports classifiés à une personne morale ;
- à cette personne morale d'exécuter de tels contrats.

La détention d'informations et supports classifiés impose aux personnes morales de disposer, en plus de l'habilitation, des aptitudes physiques des locaux et techniques des systèmes numériques homologués (selon les cas spécifiques).

Les personnes morales doivent être habilitées, au plus tard à la date de signature du contrat⁹⁶, pour l'exécution de travaux classifiés dans le cadre d'un contrat conclu avec l'autorité publique, directement ou de manière indirecte, dans le cadre des sous-traitances ou, pour les marchés publics et les concessions de défense ou de sécurité, dans le cadre des sous-contrats.

L'habilitation de la personne morale et d'un représentant légal sont un préalable indispensable à l'habilitation du personnel de la société. À l'exception toutefois :

- des phases précontractuelles nécessitant l'accès ou la détention des informations et supports classifiés pour l'établissement du contrat, pour lesquelles une ou des personnes physiques spécifiquement désignées doivent obtenir l'habilitation ;
- de celle de l'administrateur d'un système numérique de niveau *Diffusion Restreinte*, lorsqu'une habilitation est requise, dans les conditions définies par l'autorité publique contractante.

⁹⁴ Pour les entités du ministère, ces mesures sont détaillées dans le titre 5 de l'IM 1544.

⁹⁵ Le modèle de fiche est disponible sur le site Internet Armement (<https://armement.defense.gouv.fr>).

⁹⁶ En particulier si l'acheteur accorde un délai supplémentaire (cf. articles R.2343-4 et R.2343-5 du code de la commande publique).

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

En cas de non-respect de la procédure d'habilitation lors de la procédure de passation du contrat (absence de fourniture de son dossier de demande d'habilitation dans les délais fixés par l'autorité contractante, par exemple), la candidature est déclarée irrecevable. Le candidat ne peut donc plus prétendre à l'attribution du contrat.

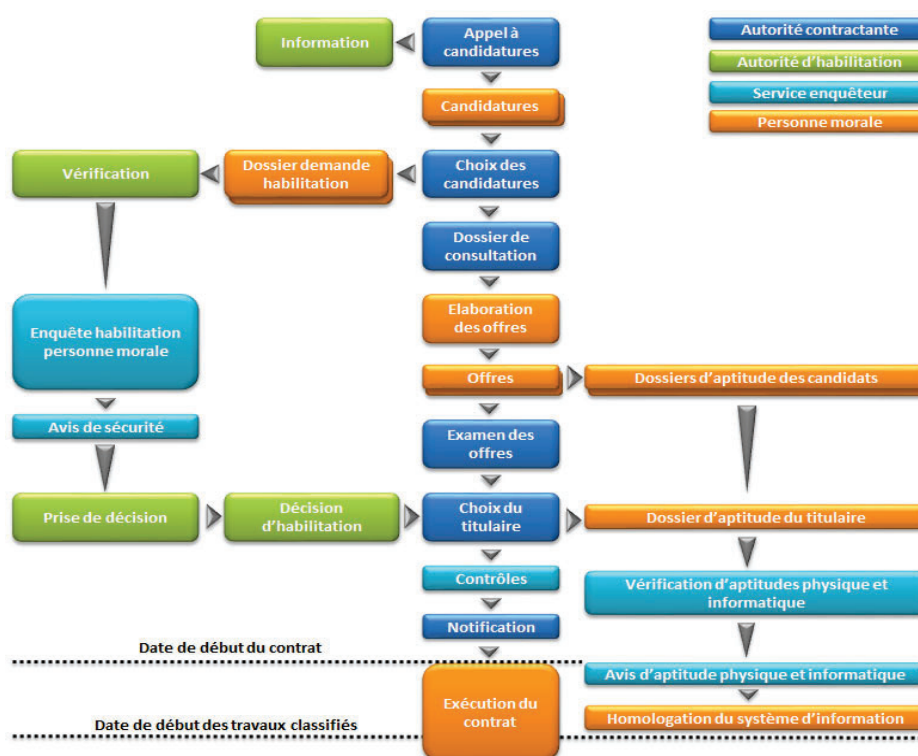
Les décisions d'habilitation délivrées à l'occasion de la passation d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés comportent une date limite de validité fixée par l'autorité d'habilitation⁹⁷ ainsi que, s'il y a lieu, un domaine particulier.

L'habilitation d'une personne morale s'accompagne pour celle-ci de la mise en place d'une structure de sécurité adaptée aux travaux classifiés qu'elle doit exécuter.

3. Simultanéité des procédures

Le schéma suivant présente de façon synthétique la synchronisation classique des processus d'achat, d'habilitation, d'aptitude et d'homologation. L'habilitation est parfois exigée dès la phase précontractuelle.

Synchronisation des procédures d'achat, d'habilitation, d'aptitude et d'homologation



Les détails de chacune des étapes figurent dans les fiches 4.4 à 4.11

⁹⁷ Cette durée d'habilitation ne peut excéder 5 ans pour le Très Secret et 7 ans pour le Secret.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.1****ACTEURS DES CONTRATS****Références :**

- Code de la défense – articles R.2311-8 et suivants.
- Code de la commande publique – articles L.6, L.1211-1 et suivants et articles L.2393-1 et suivants.
- IGI 1300 – 4.1 à 4.2, 4.4.1.2, 4.4.2.2

Points clés

- L'autorité d'habilitation délivre les décisions d'habilitation à la personne morale et aux personnes physiques qui lui sont rattachées et participent à l'exécution du contrat.
- L'autorité contractante détermine le type de contrat et ses conséquences sur la procédure contractuelle.
- En cas d'accès ou de détention d'informations et supports classifiés, la personne morale candidate doit se soumettre, si elle n'est pas déjà habilitée, si son habilitation porte sur un autre domaine que celui du contrat ou si les éléments constitutifs ont changé, à une procédure d'habilitation pour que sa candidature soit retenue.
- Le service enquêteur effectue les enquêtes d'habilitation des personnes morales et des personnes physiques et émet des avis techniques d'aptitude physique (ATAP) ou informatique (ATAI) en vue respectivement de l'aptitude des lieux abritant des informations et supports classifiés et de l'homologation des systèmes numériques.

1. L'autorité d'habilitation

L'autorité d'habilitation est l'organisme chargé de délivrer les agréments des officiers de sécurité (cf. fiche 2.3) ainsi que les décisions d'habilitation (ou de refus) des personnes morales et de leur personnel, sur la base de l'avis de sécurité émis par le service enquêteur.

Pour le *Très Secret* classification spéciale, l'autorité d'habilitation est le SGDSN⁹⁸.

Pour les habilitations de niveau *Secret* ou *Très Secret*, l'autorité d'habilitation pour toutes les personnes morales travaillant au profit du ministère de la défense et du CEA/DAM est la DGA (à l'exception des personnes morales travaillant au profit de la DGSE).

⁹⁸ Cette classification concerne exclusivement les personnes physiques.

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.1

2. L'autorité contractante

Elle désigne toute personne publique ou privée qui fait appel à un fournisseur ou à un prestataire pour l'exécution d'un contrat ou d'un marché. Lorsque le marché est régi par les dispositions du code de la commande publique, l'expression « autorité contractante⁹⁹ » désigne le pouvoir adjudicateur. En cas de contrats de sous-traitance ou de sous-contrats, la personne morale titulaire du contrat est dénommée le « primo-contractant ».

En cas de nécessité d'habilitation pour l'accès ou la détention d'informations et supports classifiés, c'est à l'autorité contractante qu'incombe :

- l'information de l'autorité d'habilitation du lancement de la procédure d'achat ;
- le choix du type de contrat (impliquant l'accès ou la détention à des informations et supports classifiés) approprié à la protection du secret de la défense nationale ;
- l'information des personnes morales candidates sur les modalités à observer pour se procurer les formulaires de constitution du dossier d'habilitation ;
- le visa des documents relatifs à la définition et à la justification du besoin d'en connaître et sa transmission à l'autorité d'habilitation ;
- la détermination, en concertation avec l'autorité d'habilitation, de la date limite de remise du dossier d'habilitation de la personne morale et du dossier d'habilitation personne physique du représentant légal¹⁰⁰ ;
- la détermination, en concertation avec l'autorité d'habilitation, de la date limite de remise des dossiers d'aptitude physique des locaux et des systèmes d'information ;
- l'autorisation ou le refus de recourir à la sous-traitance de travaux classifiés ;
- la transmission des dossiers d'habilitation à l'autorité d'habilitation ;
- la transmission des projets de plans contractuels de sécurité (PCS) aux candidats ;
- la transmission au titulaire du plan contractuel de sécurité dans le cadre du marché ;
- la mise en cohérence du plan contractuel de sécurité avec les évolutions éventuelles des autres documents constitutifs du marché.

Elle doit notamment s'assurer, si nécessaire, pour certains points ci-dessous, auprès de l'autorité d'habilitation, que :

- le projet de plan contractuel de sécurité a été établi afin de le joindre au dossier de consultation¹⁰¹ ;
- les candidats ont fourni l'attestation d'habilitation appropriée ou déposé un dossier d'habilitation ;
- pour les contrats impliquant l'accès ou la détention d'informations et supports classifiés en phase précontractuelle, que les candidats admis à soumissionner aient fait l'objet d'une décision d'habilitation ou engagé le processus d'habilitation nécessaire avant la mise à disposition des documents de la consultation nécessaire à l'élaboration de leur offre ;
- que l'attributaire pressenti ait fait l'objet d'une décision d'habilitation.

⁹⁹ Ou autorité concédante dans le cadre de l'article R.3123-3 du code de la commande publique.

¹⁰⁰ Personne ayant le pouvoir d'engager la société et inscrite au K-BIS de la société.

¹⁰¹ À l'exception des contrats cadres, pour lesquels une ébauche de plan contractuel ou un plan contractuel cadre (type PCS père-fils) est suffisante.

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.1

En fonction du type de contrat à passer (impliquant l'accès ou la détention d'informations et supports classifiés, contrat sensible), l'autorité contractante détermine les conséquences sur la procédure d'acquisition (avis d'appel à candidatures, modalités particulières de consultation, plan contractuel de sécurité, demandes d'habilitation de candidats, etc.).

Pour l'assister dans ces missions, l'autorité contractante recourt à un binôme prescripteur technique/acheteur et à son officier de sécurité.

a. Binôme prescripteur technique/acheteur

Il doit vérifier, dès l'expression du besoin, s'il existe des informations et supports sensibles, *Diffusion Restreinte* ou classifiés, ou des systèmes numériques particuliers¹⁰² à protéger :

- dans la phase précontractuelle (en particulier si le dossier de consultation comporte des éléments classifiés) ;
- dans la phase contractuelle.

Il est responsable de :

- l'identification des informations et supports à protéger ;
- l'identification des systèmes numériques de la personne morale¹⁰³¹⁰⁴ qui interviendront pour la réalisation du contrat et l'identification des mesures de sécurité spécifiques complémentaires à la présente instruction et au cadre réglementaire applicable (par exemple mesures de cloisonnement particulières). Les systèmes d'information et les mesures spécifiques de sécurité sont mentionnées au PCS. Le PCS doit être mis à jour en cas d'évolution de la liste des systèmes numériques ;
- l'élaboration de la fiche de besoin de protection du secret ;
- l'élaboration des plans contractuels de sécurité liés aux contrats impliquant l'accès ou la détention d'informations et supports classifiés dont il demande la passation ;
- l'élaboration de la fiche de suivi de passation du contrat ;
- la gestion de l'arborescence (sous-traitance) des travaux classifiés réalisés au titre du contrat.

b. Officier de sécurité de l'autorité contractante

En matière de protection des informations et supports classifiés dans les contrats, l'officier de sécurité et l'officier de sécurité des systèmes d'information conseillent le binôme prescripteur technique/acheteur et l'autorité contractante :

- sur le choix du contrat (impliquant l'accès ou la détention d'informations et supports classifiés) ;

¹⁰² Par exemple ; les Systèmes d'Information d'Importance Vitale ne contiennent pas forcément d'informations sensibles, *Diffusion Restreinte* ou classifiées mais nécessitent la mise en œuvre de mesures particulières de sécurité et doivent être identifiés avant le lancement du contrat.

¹⁰³ Voir chapitre 4.8 du présent titre.

¹⁰⁴ L'identification des Systèmes d'Information d'Importance Vitale relève de la responsabilité du contractant mais doit être effectuée avec le soutien de l'autorité contractante. Lorsque les systèmes numériques ne sont pas encore formellement déclarés comme S Systèmes d'Information d'Importance Vitale, ils peuvent être identifiés comme des candidats Systèmes d'Information d'Importance Vitale.

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.1

- pour l'élaboration du plan contractuel de sécurité et la gestion de l'arborescence des travaux classifiés réalisés au titre du contrat ;
- sur chaque intention d'achat conduisant à la communication d'informations et supports classifiés ;
- pour l'expression des besoins d'habilitation des personnes morales candidates à la passation de contrats impliquant l'accès ou la détention d'informations et supports classifiés ou détention d'informations et supports classifiés ;
- sur l'identification des systèmes numériques à mentionner dans le plan contractuel de sécurité.

En outre, il contrôle ou fait contrôler l'application des plans contractuels de sécurité aux contrats impliquant l'accès ou la détention d'informations et supports classifiés passés par l'autorité contractante.

En matière de protection des informations sensibles et *Diffusion Restreinte* et en matière de sécurité numérique, l'officier de sécurité, en concertation avec l'officier de sécurité des systèmes d'information, conseille le binôme prescripteur technique/acheteur sur les mesures de protection à mettre en œuvre dans le futur contrat.

3. La personne morale

a. Cas général des personnes morales régies par le droit privé

La personne morale peut être selon les différentes phases des procédures d'achat :

- tout d'abord candidat ;
- puis soumissionnaire ;
- attributaire ;
- et enfin titulaire.

Si le candidat n'est pas déjà habilité ou si les éléments constitutifs de la personne morale ont évolué depuis la décision d'habilitation, il doit se soumettre à la procédure d'habilitation pour que sa candidature à un contrat impliquant l'accès ou la détention d'informations et supports classifiés soit retenue ou que son offre soit examinée. Il constitue son dossier d'habilitation¹⁰⁵ en se reportant aux exigences décrites dans les documents de consultation. L'ensemble des pièces requises est envoyé simultanément.

Dans le cas de la passation d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés, le soumissionnaire¹⁰⁶ doit aussi remettre un dossier d'aptitude en vue d'apprécier sa capacité à détenir et protéger des informations et supports classifiés.

Toutes les personnes morales habilitées doivent disposer d'un officier de sécurité. Dans les établissements détenant des informations et supports classifiés, elles doivent disposer d'officiers de sécurité d'établissement, encadrés par un officier central de sécurité. Les rôles et missions de l'officier de sécurité sont précisés dans la fiche 2.5.

¹⁰⁵ Le modèle de dossier d'habilitation est accessible sur le site Armement (<https://armement.defense.gouv.fr>).

¹⁰⁶ Ce dossier n'est pas exigé au stade de la candidature.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.1****b. Cas particulier des établissements publics**

Les établissements publics administratifs (EPA) et les établissements publics industriels et commerciaux (EPIC) peuvent accéder ou détenir des informations et supports classifiés sans habilitation de la personne morale sous réserve de disposer d'un besoin d'en connaître reconnu par le ministre. Ils restent assujettis aux dispositions de la présente instruction s'agissant, notamment, des dossiers d'aptitude et des habilitations de leur personnel.

Une habilitation personne morale peut néanmoins être exigée dans le cadre d'une candidature à un appel d'offres ou un appel à projet international nécessitant l'accès à des informations et supports classifiés.

c. Cas particulier des micro-entrepreneurs ou des sociétés unipersonnelles

Dans le cadre des habilitations, le ministère de la défense considère les micro-entrepreneurs (anciennement autoentrepreneur) comme des personnes morales liées par contrat ou convention au ministère et leur applique donc la procédure d'habilitation des personnes morales décrite dans ce chapitre (avec aptitude physique ou informatique en cas de détention d'informations et supports classifiés).

La même procédure s'applique également à la SASU (société par actions simplifiée unipersonnelle).

d. Cas des groupements momentanés d'entreprises (GME)

L'exécution de certains contrats nécessite le regroupement des compétences de plusieurs entreprises au sein d'un groupement momentané d'entreprises (GME) qui constitue le titulaire du contrat. Au sein de ce groupement chaque membre, dénommé cotraitant, est une personne morale à part entière. Parmi les cotraitants, un mandataire est désigné pour les représenter auprès du maître d'ouvrage et coordonner les activités du GME.

Il existe deux formes juridiques pour un GME :

- GME conjoint : chaque entreprise membre du groupement s'engage à exécuter uniquement la partie des prestations qui lui est attribuée dans le contrat. Chaque cotraitant est responsable de sa propre part des travaux.

Il peut être imposé par le maître d'ouvrage que le mandataire soit solidaire des autres membres. Dans ce cas, seule l'entreprise mandataire est solidairement engagée pour l'ensemble du contrat et doit prendre en charge les obligations de ses cotraitants en cas de défaillance ;

- GME solidaire : chaque entreprise du groupement est solidairement engagée pour l'ensemble du contrat. Si l'un des membres est défaillant, les autres doivent prendre en charge ses obligations. Lorsque le contrat nécessite l'accès ou la détention d'informations ou supports classifiés, le mandataire d'un GME, quelle qu'en soit la forme juridique, est systématiquement habilité. Si la forme juridique du groupement est conjointe avec mandataire solidaire ou non, seuls les cotraitants nécessitant l'accès ou la détention d'informations ou supports classifiés pour l'exécution de leurs

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.1

obligations doivent être habilités. Dans le cas d'un groupement solidaire, tous les cotraitants doivent être habilités.

Le mandataire du groupement est en charge de :

- s'assurer que les cotraitants nécessitant un accès ou une détention d'informations ou supports classifiés ont effectué les démarches d'habilitation de la personne morale auprès de l'autorité contractante ;
- s'assurer que chaque cotraitant le nécessitant a fait l'objet d'une habilitation de la personne morale en vue de l'exécution de ses obligations, dans le respect des spécifications du plan contractuel de sécurité.

e. Cas des sous-traitants et des sous-contractants

Dans le cadre d'un contrat, une partie des prestations peut être sous-traitée. Le sous-traitant ou le sous-contractant doit alors être déclaré et, si nécessaire, habilité.

Dans le cadre de sous-contrats, par exemple d'achats de fournitures, le sous-contractant doit également être identifié et, si nécessaire, habilité.

La personne morale avec laquelle l'autorité contractante a conclu un contrat est qualifiée de primo contractante et est responsable des déclarations et demandes d'habilitation de tout sous-traitant et sous-contractant.

4. Le service enquêteur

Le service enquêteur est chargé d'effectuer les enquêtes d'habilitation des personnes morales, du représentant légal, du bénéficiaire effectif¹⁰⁷ et de leur personnel devant accéder ou détenir des informations et supports classifiés. Il doit se prononcer, le cas échéant, sur l'aptitude des locaux et des systèmes d'information des personnes morales et peut procéder à des visites, contrôles et inspections. À ce titre, il émet des avis de sécurité au profit de l'autorité d'habilitation et des avis techniques d'aptitude physique (ATAP) ou informatique (ATAI) au profit des autorités contractantes, de l'autorité d'habilitation et des personnes morales détenant des informations et supports classifiés.

La DGSE est, pour ses propres besoins, service enquêteur et son directeur général est autorité d'habilitation.

¹⁰⁷Le bénéficiaire effectif désigne toute personne physique détenant directement ou indirectement plus de 25% du capital ou des droits de vote de la société ou la personne qui exerce par tout moyen un pouvoir de contrôle ou de direction sur les organes de direction ou de gestion.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.2****CHOIX DU TYPE DE CONTRAT****Référence :**

- IGI 1300 – 4.4, 5.3.2

Points clés

- Les contrats impliquant l'accès ou la détention d'informations et supports classifiés comportent des clauses de protection du secret et un plan contractuel de sécurité.
- Dans le cadre d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés, l'autorité contractante est responsable de la protection de ces derniers.
- Dans le cadre d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés, la personne morale est responsable de la protection des informations et supports classifiés qu'elle détient.
- La passation d'un contrat sensible ne nécessite ni l'habilitation du candidat ni celle de son personnel. Le personnel fait cependant l'objet d'une enquête administrative. La personne morale peut également faire l'objet d'une enquête sur demande de l'autorité contractante.
- Il est également possible d'introduire des dispositions de protection dans n'importe quel type de contrat.

1. Contrat avec accès à des informations et supports classifiés

Il s'agit de tout contrat, quel que soit le régime juridique qui lui est applicable ou sa dénomination, dans lequel une personne morale, publique ou privée, est amenée, à l'occasion de la passation du contrat ou de son exécution, à avoir accès à des informations et supports classifiés sans les détenir.

L'exécution de ce contrat nécessite l'habilitation de la personne morale et de son personnel ayant à connaître des informations et supports classifiés au titre du contrat. Dûment habilitées au préalable, les personnes physiques employées par la personne morale, disposant du besoin d'en connaître, accèdent aux informations et supports classifiés sous la responsabilité de leur détenteur. L'autorité contractante reste responsable de la protection des informations et supports classifiés nécessaires à l'exécution du contrat ou produits à l'occasion de son exécution. Les aptitudes physiques des locaux ou l'homologation des systèmes d'information sont sans objet pour ce type de contrat, le candidat ou le titulaire ne détenant pas d'information et support classifié à ce titre.

Les établissements de la personne morale ayant du personnel habilité participant à l'exécution du contrat doivent être identifiés auprès de l'autorité d'habilitation et du service enquêteur.

Tout contrat avec accès à des informations et supports classifiés comporte :

- **des clauses de protection du secret** (cf. IGI 1300 – annexe 17) qui précisent les conditions de protection des informations et supports classifiés et d'exécution des travaux classifiés du contrat ;

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.2

- **un plan contractuel de sécurité** spécifique au contrat auquel il est associé dont les modalités d'élaboration et d'approbation sont précisées dans la fiche 4.8.

2. Contrat avec détention d'informations et supports classifiés

Il s'agit de tout contrat, quel que soit son régime juridique ou sa dénomination, dans lequel une personne morale, publique ou privée, est amenée à l'occasion de la passation du contrat ou de son exécution à détenir des informations et supports classifiés dans ses propres locaux.

Dans ce type de contrat, des informations et supports classifiés sont transférés ou élaborés dans un ou plusieurs établissements relevant d'une personne morale qui a l'obligation de mettre en œuvre, dans ses installations, les mesures de protection réglementaires. Elle est alors responsable de la protection des informations et supports classifiés qu'elle détient. Les personnes physiques employées par la personne morale et détenant des informations et supports classifiés au titre du contrat sont responsables de leur protection.

Un contrat avec détention d'informations et supports classifiés nécessite de remplir toutes les conditions énoncées au §1 et de détenir :

- l'attestation de conformité physique des locaux dans lesquels sont détenus des informations et supports classifiés, établie par le représentant légal de la personne morale ;
- l'homologation des systèmes d'information sur lesquels ces informations sont conservées.

3. Contrat sensible

Il s'agit de tout contrat, quel que soit son régime juridique ou sa dénomination¹⁰⁸, qui n'implique pas l'accès à des informations ou supports classifiés et dont l'exécution nécessite l'accès à un lieu abritant des éléments couverts par le secret de la défense nationale dans lequel un cocontractant de l'administration, public ou privé, prend des mesures de précaution, y compris dans les contrats de travail de ses salariés. Ces mesures tendent à assurer que les conditions d'exécution de la prestation ne mettent pas en cause la sûreté ou les intérêts essentiels de l'État¹⁰⁹.

Les contrats sensibles s'appliquent, notamment, aux prestations suivantes :

- les prestations d'entreprises de prévention et de sécurité (gardiennage, intervention, levée de doute, contrôle d'accès, détection d'intrusion, vidéosurveillance, télésurveillance, etc.) dans un local abritant des éléments couverts par le secret de défense nationale ;
- les prestations réalisées sur les éléments et réseaux de sûreté, pouvant remettre en cause l'équation de sûreté (installation et maintenance de systèmes de contrôle d'accès, de détection d'intrusion, de vidéosurveillance, etc.).

¹⁰⁸ À l'exception des contrats de travail.

¹⁰⁹ Certaines activités, intéressant la dissuasion, peuvent nécessiter des enquêtes administratives même si le contrat n'est pas un contrat classifié ou sensible.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.2**

La passation d'un contrat sensible ne nécessite ni l'habilitation du candidat ni celle de son personnel mais justifie des enquêtes administratives qui peuvent être sollicitées par l'officier de sécurité du contractant auprès du service enquêteur compétent¹¹⁰ :

- à la diligence du contractant, celle relative à la personne morale ;
- celles relatives au personnel du titulaire exécutant ce contrat, en lien avec le bénéficiaire exprimant le besoin de sécurité.

Tout contrat sensible comporte une clause type de protection du secret précisant les mesures de sécurité particulières devant être prises pour l'exécution du contrat (limite des lieux, horaires d'intervention, etc.)¹¹¹.

Lorsqu'un contrat sensible s'exécute dans une zone réservée en l'absence du personnel occupant habituellement la zone, le prestataire doit être accompagné ou surveillé par l'autorité responsable de la zone réservée.

¹¹⁰ Si l'exécution du contrat nécessite l'accès dans des zones protégées en raison des activités sensibles qui s'y exercent.

¹¹¹ Cf. annexe 33 de l'IGI 1300.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.3****MODALITÉS DE PASSATION D'UN CONTRAT SENSIBLE****Référence :**

- IGI 1300 – 5.3.2.1 et annexe 33

Points clés

- Les personnes morales soumissionnaires peuvent faire l'objet d'une enquête administrative dans le cadre d'un contrat sensible préalablement à sa passation.
- Dans tous les cas, il est procédé aux enquêtes administratives à l'endroit des personnes physiques.
- Aucune de ces enquêtes ne conduit à l'habilitation.

1. Lancement de la procédure d'achat

Pour toute procédure de passation d'un contrat sensible, le prescripteur technique évalue les mesures de protection devant être adossées au projet de contrat.

Si la sensibilité des prestations à réaliser au titre du contrat le nécessite, et après concertation entre l'officier de sécurité du contractant et le service enquêteur, une enquête administrative de la personne morale est recommandée. Dans tous les cas, les personnes physiques sont soumises à une enquête administrative.

L'acheteur, lors du lancement de la consultation, informe les candidats potentiels de la procédure d'enquête de la personne morale (le cas échéant) et des personnes physiques (dans tous les cas) devant participer aux prestations du contrat.

Les cas d'exclusion de la procédure d'achat sont précisés au paragraphe 5.3.2.2 de l'IGI 1300.

2. Traitement des enquêtes administratives de la personne morale des candidats admis à soumissionner

Si l'autorité contractante demande une enquête administrative sur la personne morale, dès qu'elle a fixé la liste des candidats admis à soumissionner, les soumissionnaires adressent à l'autorité contractante les pièces suivantes :

- les extraits du registre du commerce et des sociétés (Kbis) de moins de trois mois ;
- la fiche navette (annexe 34 de l'IGI 1300) ;
- les fiches de contrôle primaire du représentant légal de la société ;
- la notice de sécurité personne morale contrat sensible (cf. partie 1¹¹² de l'annexe 20 de l'IGI 1300) ;
- sur demande du service enquêteur : les copies des cartes d'identité ou passeports des personnes physiques clefs (gérants, actionnaires, etc. tels qu'indiqués dans le RCS) de la personne morale. Les soumissionnaires n'ayant pas remis les documents

¹¹² Seule la partie 1 « description de la personne morale » de l'annexe 20 de l'IGI 1300 est à remplir.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.3**

prévus à la date fixée sont réputés avoir renoncé à l'exécution des prestations du contrat sensible.

Pour chacun des soumissionnaires, après analyse de la complétude des pièces par l'officier de sécurité de l'autorité contractante, celui-ci transmet les éléments nécessaires à l'enquête administrative au service enquêteur en précisant la date souhaitée pour disposer des avis avant le choix de l'attributaire.

3. Choix de l'attributaire du contrat

Le résultat de l'enquête administrative menée, le cas échéant, sur chaque personne morale soumissionnaire ayant remis une offre acceptable est pris en compte pour le choix de l'attributaire.

Avant la date de choix de l'attributaire du contrat, l'autorité contractante s'assure auprès de son officier de sécurité que tous les avis d'enquête nécessaires sont disponibles à cette date. Si certains de ces avis risquent de ne pas être donnés à temps, l'acheteur et l'officier de sécurité examinent la possibilité d'adaptation des délais des procédures d'achat et de contrôle. En dernier ressort, en cas d'urgence justifiée, l'officier de sécurité, après consultation du service enquêteur, prend la décision appropriée.

Après la prise de connaissance de l'avis du service enquêteur, l'autorité contractante procède au choix de l'attributaire du contrat.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.4****PRISE EN COMPTE DE LA PROTECTION DU SECRET DANS LA
PROCÉDURE D'ACHAT****Références :**

- Code de la commande publique – articles R.2343-4 et R.2343-5
- IGI 1300 – 4.4.1

Points clés

- L'acheteur, en lien avec le prescripteur technique et l'officier de sécurité concerné, établit une fiche de suivi de passation du contrat en se basant sur l'analyse du degré de protection à accorder lors de la passation et de l'exécution du contrat figurant sur la fiche de besoin de protection du secret.
- Les contrats impliquant l'accès ou la détention d'informations et supports classifiés ne peuvent être signés qu'après réception de l'attestation d'habilitation de la personne morale retenue.

1. Expression du besoin de protection du secret

La prise en compte des besoins de protection du secret dans les phases précontractuelles puis d'exécution du contrat doit être appréhendée différemment selon la procédure d'acquisition envisagée.

Pour toute procédure de passation devant aboutir à un contrat impliquant l'accès ou la détention d'informations et supports classifiés, le prescripteur technique doit préciser avec le concours de son officier de sécurité, lors de la demande d'achat, le besoin de protection du secret concernant la phase précontractuelle et l'exécution du contrat. Si nécessaire, ce dernier consulte l'autorité d'habilitation.

L'expression de ce besoin fait l'objet d'une fiche de besoin de protection du secret¹¹³. Cette fiche doit impérativement être jointe à la demande d'achat.

Les renseignements relatifs au type de contrat et à la procédure d'acquisition retenus par l'acheteur, en lien avec le prescripteur technique et l'officier de sécurité concerné, sont portés sur la fiche de suivi de passation du contrat qui sera transmise à l'autorité d'habilitation.

Si les informations font l'objet de la mention *Spécial France*, le service prescripteur consulte l'officier de sécurité ou l'autorité d'habilitation pour déterminer les dispositions les plus appropriées associées à l'utilisation de cette mention de protection.

¹¹³ Un modèle de fiche de besoin de protection du secret est disponible sur le site Internet Armement (<https://armement.defense.gouv.fr>).

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.4

2. Habilitations ou aptitudes et homologations nécessaires

L'autorité contractante ne peut signer aucun contrat impliquant l'accès ou la détention à des informations et supports classifiés avant la réception de l'attestation d'habilitation de la personne morale.

Lorsque le contrat implique :

- la détention d'informations et supports classifiés : cette dernière ne peut débiter avant l'obtention de l'aptitude physique au niveau requis ;
- l'usage d'un système numérique soumis à la présente instruction : l'exécution des travaux liés au système numérique ne peut débiter avant la date d'homologation de ce système (cf. fiche 6.2).

Pour un contrat impliquant la détention d'informations et supports classifiés, au stade de sa candidature, la personne morale transmet, parallèlement au dossier d'habilitation, un engagement à déposer, au titre de son offre, un dossier d'aptitude¹¹⁴.

Au stade de la remise de son offre, le soumissionnaire dépose un dossier d'aptitude (allégé ou complet, cf. fiche 4.5. §3) pour chacun de ses locaux ou système numérique destinés à traiter des informations et supports classifiés.

Si le titulaire du marché avec détention d'informations et supports classifiés fait l'objet d'un avis d'inaptitude, l'autorité contractante peut prendre les sanctions adéquates, allant jusqu'à la résiliation du marché à ses torts.

Pour un marché de défense ou de sécurité, lorsqu'un candidat n'est pas habilité au moment de sa candidature à la passation d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés, l'autorité contractante peut accorder un délai supplémentaire à ce candidat pour obtenir cette habilitation¹¹⁵.

Pour les marchés autres que ceux de défense ou de sécurité, à l'exception des marchés passés en vertu de l'article L.2512-3 du code de la commande publique, le fait pour un candidat de ne pas être habilité au moment de sa candidature à la passation d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés ne constitue pas une raison suffisante pour justifier *a priori* son exclusion de la procédure de passation de ce contrat.

Dans tous les cas, s'il y a refus de se soumettre à la procédure d'habilitation lors de la procédure de passation du contrat (absence de fourniture de son dossier d'habilitation dans les délais fixés par l'autorité contractante par exemple), le candidat est exclu de la procédure de passation de ce contrat.

¹¹⁴ Le candidat s'engage à déposer un dossier d'aptitude puis le soumissionnaire dépose un dossier d'aptitude. Le marché peut être attribué puis notifié.

¹¹⁵ Article R.2343-5 du code de la commande publique.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.5****PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT
L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS
CLASSIFIÉS : SÉLECTION DES CANDIDATS ADMIS À
SOUMISSIONNER ET CONTENU DES OFFRES****Référence :**

- IGI 1300 – 4.4.1.3, 4.4.1.5

Points clés

- Après examen de la validité des habilitations des candidats ou des demandes en cours par l'autorité d'habilitation, l'autorité contractante établit la liste des candidats admis à soumissionner.
- Un dossier de consultation, établi par l'acheteur, est adressé aux candidats admis à soumissionner. Il inclut le projet de plan contractuel de sécurité.
- Les dossiers d'aptitude des locaux et des systèmes numériques sont établis par la personne morale pour les contrats impliquant l'accès ou la détention d'informations et supports classifiés.

1. Lancement de la procédure d'achat

Pour toute procédure de passation d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés, l'acheteur établit, en liaison avec le prescripteur technique et l'officier de sécurité de l'autorité contractante, la fiche de suivi de passation du contrat¹¹⁶. Cette fiche est transmise à l'autorité d'habilitation.

L'acheteur fournit à l'autorité d'habilitation les dates prévisionnelles de choix de l'attributaire et de notification du contrat (ou éventuellement de mise à disposition des informations et supports classifiés si cette date est notablement différente de celle de la notification du contrat).

En cas de procédure avec publicité, l'acheteur établit l'avis d'appel public à la concurrence (AAPC), qui précise les modalités et conditions de participation à la consultation, notamment :

- pour les candidats non habilités, les informations relatives à la constitution et au dépôt d'un dossier d'habilitation ;
- pour les candidats déjà habilités, la production d'attestations d'habilitation accompagnées d'une attestation de non changement de la personne morale depuis la dernière décision d'habilitation ou un justificatif prouvant que les démarches de mise à jour de l'habilitation ont été entreprises auprès de DGA/SSDI ou d'une autre autorité d'habilitation (cf. fiche 4.11) ;

¹¹⁶ Le modèle de fiche de suivi de passation du contrat est disponible sur le site Internet Armement (<https://armement.defense.gouv.fr>).

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.5**

- le niveau et la nature des travaux classifiés à réaliser ainsi que le niveau et la nature de l'habilitation de la personne morale candidate ;
- en cas de contrat impliquant la détention d'informations et supports classifiés, le niveau et la nature des aptitudes à détenir et un engagement à fournir un dossier d'aptitude ;
- les destinataires des pièces constitutives du dossier de candidature.

Pour une procédure sans publicité, l'acheteur établit une lettre d'invitation à participer à une consultation en y faisant apparaître les mêmes éléments que cités *supra* dans le cadre de l'avis d'appel public à la concurrence et en fonction de la fiche de suivi de passation du contrat.

Dans le dossier de consultation établi en vue de la passation d'un contrat impliquant la détention d'informations et supports classifiés, l'acheteur fait connaître à chaque candidat admis à soumissionner qu'il doit adresser en même temps que son offre un dossier d'aptitude pour chaque établissement dans lequel il envisage de réaliser des travaux classifiés au titre du contrat et procéder à l'homologation des systèmes numériques susceptibles d'héberger des informations et supports classifiés.

Si le dossier de consultation comporte des éléments classifiés, l'acheteur fait prendre les dispositions décrites dans la fiche 4.6.

Si le contrat en cause est un marché de défense ou de sécurité, conformément aux articles R.2343-4 et R.2343-5 du code de la commande publique, l'autorité contractante doit exiger que les candidats soient habilités dès le dépôt des candidatures. Elle peut cependant accorder aux candidats qui ne sont pas habilités au moment du dépôt de leur candidature un délai supplémentaire pour obtenir cette habilitation. Elle indique ce délai dans l'avis d'appel à la concurrence.

2. Choix des candidatures

L'autorité contractante adresse à l'autorité d'habilitation, *via* son officier de sécurité, la liste des candidats accompagnée des éléments relatifs à leur habilitation ou des documents nécessaires au dépôt d'une demande d'habilitation. Après examen des éléments transmis, et selon le contexte, l'autorité d'habilitation :

- certifie à l'autorité contractante que les candidats disposent effectivement des habilitations requises ;
- informe l'autorité contractante de la complétude des informations transmises permettant de lancer un dossier d'habilitation ;
- ou informe l'autorité contractante que les dossiers déposés sont incomplets et que des éléments complémentaires sont nécessaires pour admettre le candidat à soumissionner.

L'autorité contractante établit la liste des candidats admis à soumissionner, en tenant compte des éléments fournis par l'autorité d'habilitation après examen des attestations d'habilitation ou de la complétude des demandes d'habilitation.

Lorsque les dossiers sont complets, l'autorité d'habilitation engage la procédure d'habilitation des candidats admis à soumissionner en transmettant au service enquêteur les dossiers d'habilitation des candidats concernés en vue de l'établissement d'un avis de sécurité.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.5****3. Dossier de consultation**

L'acheteur adresse le dossier de consultation aux candidats retenus. Si le dossier de consultation ne comporte aucune information et support classifié, il est transmis à tous les candidats admis à soumissionner, qu'ils soient habilités ou non. Si le dossier de consultation comporte des éléments classifiés, les dispositions de la fiche 4.6 doivent être appliquées.

Le contrat devant comporter un plan contractuel de sécurité, le projet de plan contractuel de sécurité est élaboré sous le contrôle du prescripteur technique, avec le concours de l'officier de sécurité. Ce projet est joint au dossier de consultation.

Dans le cas d'un contrat impliquant la détention d'informations et supports classifiés, en plus du dossier d'identification pour chaque établissement dont le personnel doit participer aux travaux classifiés au titre du contrat, l'acheteur indique les documents nécessaires à la constitution du dossier d'aptitude. Ces documents doivent être fournis avec l'offre dans les délais fixés dans le règlement de la consultation. Ils peuvent prendre deux formes :

- un dossier d'aptitude complet si la personne morale envisage de réaliser les travaux classifiés dans un local n'ayant pas au préalable fait l'objet d'avis d'aptitude sans objection et sur un système numérique non homologué, ou si le local et le système numérique ont fait l'objet de modifications rendant caducs les avis d'aptitude et les homologations précédemment émis ;
- un dossier d'aptitude allégé comprenant les copies des avis d'aptitude déjà obtenus, accompagnés des attestations de conformité et des homologations des systèmes numériques déjà émises, si la personne morale envisage de faire les travaux classifiés du contrat dans des locaux ayant précédemment fait l'objet d'avis techniques d'aptitude physique et sur des systèmes numériques homologués¹¹⁷.

4. Contenu des offres au regard de la protection du secret

Le candidat doit remettre à l'autorité contractante dans son offre :

- dans le cas d'un contrat impliquant l'accès à des informations et supports classifiés, un dossier d'identification pour chaque établissement dont le personnel intervient dans les travaux classifiés du contrat ;
- dans le cas d'un contrat avec détention d'informations et supports classifiés, en plus du dossier précité pour les contrats impliquant l'accès à des informations et supports classifiés, un dossier d'aptitude¹¹⁸ pour chaque établissement dans lequel sont envisagés les travaux classifiés du contrat ainsi que la liste des systèmes numériques destinés à héberger des informations et supports classifiés et pour lesquels une décision d'homologation devra être émise.

¹¹⁷ La personne morale doit accompagner ce dossier d'un engagement de non changement des conditions ayant conduit à l'obtention des avis techniques d'aptitude physique et des homologations.

¹¹⁸ Si la personne morale dispose déjà de locaux aptes et de systèmes numériques homologués et si les travaux classifiés du futur contrat doivent y être réalisés, alors son officier de sécurité établit les certificats de conformité des locaux tels que décrits dans l'annexe 26 de l'IGI 1300 et produit les décisions d'homologation correspondantes.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.6****PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT
L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS
CLASSIFIÉS : CONSULTATION DES INFORMATIONS ET SUPPORTS
CLASSIFIÉS DURANT LA PÉRIODE D'ÉLABORATION DES OFFRES****Référence :**

- IGI 1300 – 4.4.1.3

Points clés

- Les personnes morales candidates admises à soumissionner non habilitées ne peuvent se voir confier des informations et supports classifiés contenus dans le dossier de consultation des entreprises (DCE).
- Cependant, lorsque leur connaissance est nécessaire pour établir une offre et à condition que la procédure d'habilitation de la personne morale soit engagée, l'accès aux informations et supports classifiés du dossier de consultation des entreprises peut être autorisé à un nombre limité de personnes habilitées.
- Lorsque les exigences d'aptitude physique des locaux ou l'absence d'homologation des systèmes numériques des candidats ne permettent pas l'étude des informations et supports classifiés du dossier de consultation des entreprises sur place, celle-ci est effectuée dans les locaux de l'autorité contractante.

1. Principes généraux

Lorsque le dossier de consultation comporte des informations et supports classifiés dont les candidats admis à soumissionner doivent avoir connaissance pour établir leurs offres, les dispositions décrites ci-après doivent être prises en compte.

Il convient tout d'abord de séparer les éléments classifiés de ceux qui ne le sont pas.

Il est formellement interdit de confier des informations et supports classifiés à un candidat admis à soumissionner non habilité.

Il est formellement interdit de confier des informations et supports classifiés à un candidat admis à soumissionner et habilité dont les locaux n'ont pas l'aptitude physique requise ou qui ne dispose pas d'un système numérique homologué.

Il est toutefois possible de donner accès à des informations et supports classifiés au personnel d'une personne morale non encore habilitée, soumissionnaire à un contrat impliquant l'accès ou la détention d'informations et supports classifiés dont la connaissance leur est nécessaire pour établir leur offre, sous réserve que :

- la procédure d'habilitation de la personne morale soit engagée auprès du service enquêteur ;
- le personnel concerné soit habilité.

Une procédure d'habilitation d'urgence (cf. fiche 3.2. §3. a.) peut être engagée par l'autorité d'habilitation pour un nombre de personnes physiques strictement limité à ce seul besoin. Les informations et supports classifiés, ne pouvant être transmis à la

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.6**

personne morale candidate non habilitée, sont consultés dans les locaux de l'autorité contractante par du personnel habilité. Un soin particulier doit être pris pour éviter que la présence dans les locaux de l'autorité contractante du personnel d'une personne morale candidate ne conduise à une inégalité de traitement entre les candidats. La mise en œuvre de cette disposition incombe au prescripteur technique avec le concours de son OS.

La transmission d'informations et supports classifiés (cf. fiche 7.8) à un candidat admis à soumissionner et habilité doit suivre la procédure réglementaire.

2. Obligations de l'autorité passant un contrat dans lequel tout ou partie des documents de consultation sont classifiés

L'acheteur tient compte, pour la fixation des délais de remise des offres, du délai d'obtention de l'habilitation des personnes physiques devant accéder aux informations et supports classifiés du dossier de consultation des entreprises et, le cas échéant, du délai du contrôle d'aptitude des locaux et de l'homologation des systèmes d'information si ceux-ci doivent héberger des informations et supports classifiés.

Lorsque le dossier de consultation comporte des informations et supports classifiés dont les candidats admis à soumissionner doivent avoir connaissance pour établir leurs offres, l'officier de sécurité de l'autorité contractante doit :

- vérifier l'habilitation des personnes morales : niveau/nature, durée d'habilitation¹¹⁹ ;
- lancer la procédure d'habilitation pour les personnes morales ne disposant pas des habilitations requises par la consultation ;
- vérifier, lorsqu'il y a détention d'informations et supports classifiés, les aptitudes physiques des locaux des personnes morales ;
- vérifier, lorsqu'il y a détention d'informations et supports classifiés, l'homologation des systèmes d'information de la personne morale destinés à héberger des informations et supports classifiés ;
- s'assurer que seul le personnel habilité des personnes morales accède aux informations et supports classifiés ;
- s'assurer de la destruction ou de la restitution des informations et supports classifiés des candidats dont l'offre n'est pas retenue.

3. Obligations de la personne morale répondant à un contrat dans lequel tout ou partie des documents de consultation sont classifiés

Lorsque le dossier de consultation comporte des informations et supports classifiés dont la personne morale doit avoir connaissance pour établir l'offre, le candidat admis à soumissionner s'engage à :

- apporter la preuve de son habilitation au bon niveau/nature, soit au travers d'un certificat de sécurité fourni par l'autorité ayant délivré l'habilitation, soit à l'issue de la procédure d'habilitation initiée auprès de l'autorité d'habilitation ;

¹¹⁹ Si l'habilitation arrive à son terme, s'assurer de la prorogation de l'habilitation (12 mois maximum) auprès de l'autorité d'habilitation.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.6**

- apporter la preuve, lorsqu'il y a détention d'informations et supports classifiés, des aptitudes physiques de l'établissement concerné ;
- apporter la preuve, lorsqu'il y a détention d'informations et supports classifiés, de l'homologation des systèmes d'information destinés à héberger des informations et supports classifiés ;
- s'assurer que seul du personnel habilité de la personne morale accède aux informations et supports classifiés ;
- détruire ou restituer les informations et supports classifiés à leur émetteur dès la notification du rejet de l'offre de la personne morale, selon des modalités définies par l'autorité contractante.

Ces dispositions sont explicitement intégrées au dossier de consultation des entreprises.

Si la personne morale ne dispose pas de locaux aptes ni de systèmes numériques homologués, son officier de sécurité peut demander que la consultation des informations et supports classifiés se fasse dans les locaux de l'autorité contractante. Si cela n'est pas possible, la communication de ces documents se révélant indispensable, un contrôle de l'aptitude des locaux et l'homologation des systèmes numériques sont effectués au préalable. Dans ce cas, il est nécessaire de prendre contact avec l'autorité d'habilitation et le service enquêteur afin de réaliser ces opérations le plus tôt possible¹²⁰.

¹²⁰ Cette démarche est à accomplir en respectant les prescriptions de l'article R.2351-1 du code de la commande publique : « l'acheteur fixe les délais de réception des offres en tenant compte de la complexité du marché et du temps nécessaire aux opérateurs économiques pour préparer leur offre ». L'égalité de traitement des candidats est respectée.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.7****PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT
L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS
CLASSIFIÉS :
EXAMEN DES OFFRES, CHOIX DE L'ATTRIBUTAIRE ET SIGNATURE****Référence :**

- IGI 1300 – 4.4.2.1

Points clés

- En fonction des éléments fournis par l'autorité d'habilitation, l'autorité contractante sélectionne les offres conformes.
- Le début des travaux classifiés dans le cadre de contrats impliquant la détention d'informations et supports classifiés est soumis à l'avis technique d'aptitude physique du service enquêteur et à l'homologation des systèmes d'information (cf. fiche 5.7).
- Lorsque des carences de protection physique ou informatique sont constatées à la suite des avis d'aptitude émis par le service enquêteur, la personne morale dispose d'un délai fixé par l'autorité contractante pour se mettre en conformité avant le début des travaux classifiés.

1. Examen des offres et décision d'habilitation

Lorsque l'administration a accordé un délai pour obtenir l'habilitation, en vertu du code de la commande publique, pendant les périodes d'élaboration et d'examen des offres, le service enquêteur instruit les dossiers d'habilitation des personnes morales candidates admises à soumissionner¹²¹ sollicités par l'autorité d'habilitation. Sur la base des avis de sécurité qui sont émis, l'autorité d'habilitation établit la décision d'habilitation ou de refus de la personne morale retenue pour exécuter le contrat¹²² et avertit l'autorité contractante.

2. Choix de l'attributaire du contrat et signature

L'autorité contractante s'assure auprès de l'autorité d'habilitation, avant l'envoi des lettres de rejet, que toutes les personnes concernées par son exécution puissent être habilitées. Si certaines de ces décisions risquent de ne pas être prises à temps, l'acheteur et l'autorité d'habilitation examinent la possibilité d'adaptation des délais des procédures d'achat et d'habilitation. En dernier ressort, en cas d'urgence dûment justifiée, l'autorité d'habilitation, après consultation du service enquêteur, prend la décision appropriée sans le résultat définitif de l'enquête, à condition que la personne morale ait déjà fait l'objet d'une habilitation et qu'aucun changement dans la direction,

¹²¹ Il convient de porter une attention au délai nécessaire à l'enquête d'habilitation. En effet, l'émission d'un avis de sécurité par le service enquêteur peut prendre plusieurs mois.

¹²² L'habilitation peut être soumise à conditions : émise pour une activité, un contrat spécifique ou une durée limitée.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.7**

les statuts ou l'actionnariat ne soit survenu depuis la précédente habilitation. Cette consultation à caractère urgent ne peut être qu'informelle, l'avis de sécurité formel n'étant rendu qu'à l'issue d'une enquête de sécurité complète. L'habilitation émise est provisoire et ne peut excéder six mois.

Si l'attributaire pressenti fait l'objet d'un refus d'habilitation, le contrat peut alors être attribué au soumissionnaire suivant dans l'ordre de classement des offres reçues sous réserve qu'il soit habilité.

3. Vérification d'aptitude du titulaire à exécuter des travaux classifiés

Tout titulaire d'un contrat impliquant la détention d'informations et supports classifiés met en œuvre les dispositions réglementaires et les clauses contractuelles de protection des informations et supports classifiés liées à ce contrat.

Dès le choix du titulaire, l'autorité contractante informe l'autorité d'habilitation qui transmet le dossier d'aptitude du candidat retenu au service enquêteur. Ce service émet des avis techniques d'aptitude physique et informatique¹²³ (cf. fiches 5.7 et 6.3) dès que les procédures et les moyens de protection requis pour la conservation et le traitement des informations et supports classifiés sont en place. Les avis d'aptitude sont adressés au titulaire.

Les prestations classifiées attendues peuvent débuter dès lors que le service enquêteur a adressé des avis sans objection au titulaire du contrat et que, lorsque nécessaire, l'homologation des systèmes numériques concernés a été prononcée.

Il incombe à l'officier de sécurité de l'autorité contractante de vérifier le respect des procédures générales de protection du secret mises en œuvre par la personne morale (cf. fiche 4.13). Lorsque ce n'est pas le cas, la personne morale peut voir sa décision d'habilitation abrogée. L'autorité contractante est alors tenue d'examiner la nécessité ou non de mettre fin au contrat.

4. Habilitation des personnes morales en cas de groupement d'entreprises

Lorsqu'ils ne détiennent pas toutes les compétences nécessaires à l'exécution d'un contrat de la commande publique, les candidats peuvent également s'unir en groupement d'entreprises pour participer à une procédure de passation.

Deux formes de groupement sont possibles dans le code de la commande publique : le groupement conjoint et le groupement solidaire d'entreprises. Ces deux formes de groupement d'entreprises n'entraînent pas les mêmes conséquences en termes d'habilitation. Si le code de la commande publique exige la désignation d'un mandataire pour les deux formes de groupements lors de l'exécution contractuelle, il ne s'agit que d'une faculté pour la présentation de leurs candidatures ou de leurs offres.

¹²³ L'aptitude informatique est un des éléments contribuant à la constitution des dossiers d'homologation des systèmes d'information.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.7****a. Habilitation des cotraitants d'un groupement conjoint d'entreprises**

Dans un groupement conjoint d'entreprises, chaque cotraitant est responsable des prestations qui lui sont dévolues et qui doivent être expressément détaillées dans le contrat. Mais l'une d'entre elles reçoit le pouvoir de représenter les autres par mandat simple ou solidaire pour l'exécution contractuelle :

- Mandat simple : cette personne morale est mandataire du groupement conjoint et, à ce titre, est l'interlocuteur unique de l'autorité contractante. Dès lors, seul ce mandataire ainsi que les entreprises en charge expressément et spécifiquement des prestations nécessitant l'accès ou la détention d'informations et supports classifiés doivent obtenir l'habilitation pour exécuter les prestations classifiées.

En revanche, ce mandataire (simple) ne peut être tenu responsable du non-respect des obligations contractuelles des autres cotraitants, à moins qu'aucune stipulation contractuelle ne permette d'être certain qu'il n'avait pas en charge les prestations non exécutées.

- Mandat solidaire : cette personne morale est également mandataire du groupement conjoint et l'interlocuteur unique de l'autorité contractante. Seul ce mandataire ainsi que les entreprises en charge expressément et spécifiquement des prestations nécessitant l'accès ou la détention d'informations et supports classifiés doivent obtenir l'habilitation pour exécuter les prestations classifiées.

En revanche, étant solidairement responsable des autres cotraitants, ce mandataire (solidaire) peut être tenu responsable du non-respect des obligations contractuelles des autres cotraitants.

b. Habilitation des cotraitants d'un groupement solidaire d'entreprises

Dans un groupement solidaire d'entreprises, l'une d'elles doit également être mandataire des autres cotraitants et est l'interlocuteur unique de la personne publique lors de l'exécution contractuelle. Cependant, toutes les entreprises étant solidaires, elles doivent toutes obtenir l'habilitation pour exécuter les prestations classifiées. Bien que les prestations soient individualisées, n'importe laquelle des entreprises du groupement solidaire peut être tenue responsable du non-respect des obligations contractuelles des autres cotraitants.

c. Cas particuliers des informations et supports classifiés nécessaires à la constitution des offres

Si le dossier de consultation comporte des éléments classifiés, l'acheteur fait prendre les dispositions décrites dans la fiche 4.6.

Quelle que soit la forme du groupement, conjoint ou solidaire, les cotraitants peuvent choisir de présenter leurs candidatures ou leurs offres séparément pour les prestations qui leur seront dévolues, ou ensemble par le biais d'un mandataire qu'ils désignent au préalable avant la phase candidature ou avant la phase offre :

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.7**

- s'ils présentent leurs offres de façon séparée, seuls les cotraitants concernés par les prestations classifiées qui leur seront dévolues doivent être habilités afin de pouvoir constituer leurs offres ;
- si le groupement désigne un mandataire pour présenter leurs candidatures ou leurs offres, les cotraitants concernés par les prestations classifiées qui leur seront dévolues doivent être habilités au même titre que ce mandataire afin de pouvoir constituer leurs offres.

Le dossier de consultation des entreprises (DCE) doit prendre en compte ces éléments afin que seules les entreprises concernées par l'accès aux informations et supports classifiés nécessaires à la constitution de leur offre soient préalablement habilitées.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.8****PROCÉDURE D'ACHAT POUR LES CONTRATS IMPLIQUANT
L'ACCÈS OU LA DÉTENTION D'INFORMATIONS ET SUPPORTS
CLASSIFIÉS :
PLAN CONTRACTUEL DE SECURITÉ****Références :**

- IGI 1300 – 4.4.2.3.a et annexe 28
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Le plan contractuel de sécurité accompagne le contrat et décrit les mesures de protection requises pour l'exécution du contrat.
- L'autorité contractante contrôle l'ensemble des activités de protection des informations et supports classifiés, qu'il s'agisse de celles effectuées par le primo-contractant ou par ses sous-contractants.
- Chaque sous-contractant doit établir un plan contractuel de sécurité avec son contractant. Ce dernier tient à jour l'arborescence des travaux classifiés pour faciliter le contrôle de la protection des informations et supports classifiés.
- La fin d'exécution des travaux objets du plan contractuel de sécurité fait l'objet d'une fiche de clôture du PCS (FICPCS).

1. Principes

Le plan contractuel de sécurité¹²⁴ est un document contractuel qui détermine les mesures de protection nécessaires à appliquer dans le cadre du contrat auquel il est rattaché. Il est négocié dans la limite des exigences de la réglementation. Il est éventuellement classifié.

La signature du plan contractuel de sécurité doit intervenir au plus tard à la signature du contrat afin d'inscrire l'engagement de la personne morale en matière de protection du secret.

Il porte sur les prescriptions mentionnées en annexe 28 de l'IGI 1300 et a pour objectif d'énumérer les instructions de sécurité relatives au contrat et d'identifier les informations et supports classifiés ainsi que leur niveau de classification et les lieux d'exécution des différentes phases des travaux classifiés.

Il permet également d'identifier les systèmes d'information que les contractants exploitent pour l'exécution du contrat, quel qu'en soit le niveau de classification, et le cas échéant, des mesures de sécurité spécifiques qui leur sont applicables.

¹²⁴ Le plan contractuel de sécurité, tel que défini à l'article R.2311-9 du code de la défense, est la nouvelle appellation de l'annexe de sécurité. Un modèle est disponible sur le site Internet Armement (<https://armement.defense.gouv.fr>) accompagné d'un guide d'aide à son élaboration.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.8**

Il est également nécessaire lorsque le contractant possède ou manipule au titre du contrat des articles contrôlés de la sécurité des systèmes d'information, qu'ils soient classifiés ou non.

Il permet au service enquêteur d'exercer ses missions de conseil et de contrôle dans le cadre des contrats et des sous-contrats qui en découlent.

Il engage :

- l'autorité contractante, responsable de la définition du niveau de protection des informations et supports classifiés et des articles contrôlés de la sécurité des systèmes d'information (ainsi que de leurs conditions d'emploi, d'utilisation et du contrôle de l'établissement du plan contractuel de sécurité dans le cas d'un contrat passé par l'administration) ;
- le titulaire (contractant), responsable de l'identification des systèmes numériques concernés et de l'application des mesures de protection :
 - o au sein de ses établissements,
 - o par ses sous-contractants, vis-à-vis desquels il est responsable de la définition du secret des travaux sous-traités et de l'établissement du plan contractuel de sécurité de sous-contractant ;
- le sous-contractant, responsable de l'application des mesures de protection dans ses établissements. Il assume lui-même les responsabilités d'un contractant s'il sous-traite une partie de ses travaux classifiés.

Le plan contractuel de sécurité, dont le plan-type est mis à disposition par la DGA, comprend notamment :

- la liste des participants et des lieux d'exécution en appendice ;
- un cahier des prescriptions de protection du secret (CPPS) ;
- une page des signatures (selon le rang : autorité contractante et son officier de sécurité, titulaire et son officier de sécurité, sous-contractant, fournisseurs, etc.) ;
- la liste des systèmes numériques permettant l'exécution des contrats et le cas échéant les mesures spécifiques de sécurité qui leur sont applicables ;
- la fiche de clôture de plan contractuel de sécurité (FICPCS).

Un plan contractuel de sécurité peut également être établi dans le cadre :

- de travaux dont l'exécution est confiée par l'autorité contractante à un organisme appartenant au ministère de la défense ;
- d'études, développements et fabrications sur fonds privés utilisant les acquis des contrats cités au présent titre ou susceptibles de générer des informations classifiées ou non classifiés. Il n'existe pas de contrat *stricto sensu* dans ce cas. Les obligations des personnes morales découlent des seules dispositions législatives et réglementaires relatives à la protection du secret ;
- de conventions.

2. Élaboration du plan contractuel de sécurité

Le plan contractuel de sécurité est établi dès la phase préparatoire du lancement de la consultation, lorsque le caractère secret des prestations du contrat impliquant l'accès ou la détention d'informations et supports classifiés ou la présence de système numérique classifié est confirmé, et afin de permettre :

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.8**

- d'une part, la protection de ces informations le plus tôt possible ;
- d'autre part, l'appréciation par les candidats des exigences de sécurité liées à l'exécution du contrat envisagé, le coût des mesures de protection et le calendrier de leur réalisation, afin de déterminer les dispositions utiles de protection à mettre en place dès le début des travaux classifiés.

Un plan contractuel de sécurité reste applicable tant qu'il n'est pas remplacé par un autre plan contractuel de sécurité ou qu'il ne fait pas l'objet d'une fiche de clôture de plan contractuel de sécurité.

3. Identification, approbation et diffusion

Outre les références au contrat auquel il se rapporte, le plan contractuel de sécurité est identifié selon les quatre éléments suivants¹²⁵ :

- le code de l'opération protégée (OP) constitué d'une lettre et de 5 chiffres. La lettre, spécifique à une autorité contractante, est attribuée par le service enquêteur ;
- le numéro du plan contractuel de sécurité composé de 5 chiffres indiquant notamment le niveau de sous-traitance. Celui-ci est identifiable grâce au 3^{ème} chiffre : 0 pour les primo-contractants, 1 pour une sous-traitance de 1^{er} niveau, 2 pour une sous-traitance de 2^{ème} niveau, etc. ;
- l'indice de modification (A pour une première version, puis B, C, D, etc.) en fonction des changements effectués sur la première page ou dans le corps du CPPS du PC ;
- la date de l'indice qui doit être actualisée à chaque changement d'indice.

L'autorité contractante de référence est responsable, via son officier de sécurité, de l'identification des plans contractuels de sécurité établis par elle-même et des plans contractuels de sécurité de sous-contractants qui en découlent.

Les PCS sont contresignés par le titulaire du contrat et l'autorité contractante¹²⁶. Ils sont approuvés par l'officier de sécurité de l'autorité contractante après visa du prescripteur technique.

L'autorité contractante diffuse le plan contractuel de sécurité aux acteurs identifiés par celui-ci ainsi qu'au service enquêteur. Sur demande, l'autorité contractante transmet le plan contractuel de sécurité à l'autorité d'habilitation.

4. Gestion des plans contractuels de sécurité et conservation

La gestion des plans contractuel de sécurité comprend :

- la gestion des contrats auxquels sont associés les plans contractuels de sécurité ;
- le suivi des modifications des plans contractuels de sécurité ;
- la prise en compte des FICPCS.

Au titre du plan contractuel de sécurité, chaque autorité contractante :

- établit et tient à jour la liste des contrats en cours, notifiés par elle, ainsi que ceux passés en sous-contractant ;

¹²⁵ À l'exception du CEA/DAM, qui applique sa propre nomenclature.

¹²⁶ Il s'agit de l'autorité contractante dans le cas d'un PCS père. Les PCS fils conclus dans le cadre de sous-traitance ou d'un sous-contrat sont contresignés par la personne morale à l'origine de cette sous-traitance ou de ce sous-contrat.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.8**

- s'assure que chacun de ses contrats impliquant l'accès ou la détention d'informations et supports classifiés comporte un plan contractuel de sécurité approuvé au plus tard à la signature du contrat ;
- adresse semestriellement au service enquêteur et à l'autorité d'habilitation un état récapitulatif des contrats qu'elle notifie (modèle de fiche signalétique disponible sur le site Armement). Cet état peut être transmis par voie électronique sécurisée.

L'historique des contrats¹²⁷ est conservé pendant dix ans par l'autorité contractante et trois ans par le service enquêteur.

5. Arborescence des travaux classifiés

La complexité de certains programmes et la diversité des spécialités nécessitent la participation de nombreuses personnes morales qui interviennent à différents niveaux des études et des réalisations.

L'autorité contractante, avec l'appui de son officier de sécurité et de son officier de sécurité des systèmes d'information, a la charge du contrôle de l'ensemble des activités visant la protection des informations et supports classifiés, quel que soit le rang du sous-contractant. Ils doivent en particulier s'assurer que chaque titulaire de contrat nécessitant l'accès ou la détention d'informations et supports classifiés autorisé à sous-traiter des travaux classifiés a établi un plan contractuel de sécurité spécifique à ces travaux classifiés sous-traités et doit approuver explicitement ce plan contractuel de sécurité.

Pour que l'autorité contractante, l'autorité d'habilitation et le service enquêteur soient en mesure de contrôler la protection des informations et supports classifiés quel que soit le rang du sous-contractant, une arborescence des travaux classifiés doit être tenue à jour en permanence par l'autorité contractante.

Cette arborescence met en évidence, aux divers rangs de sous-contractants, les liens contractuels entre chaque titulaire et ses sous-contractants.

Le titulaire d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés ne peut communiquer à ses sous-contractants que les informations et supports classifiés décrits dans le plan contractuel de sécurité de sous-contractant approuvé par l'officier de sécurité de l'autorité contractante.

6. Modification et clôture du plan contractuel de sécurité

Un plan contractuel de sécurité peut être modifié au cours de l'exécution du contrat, à l'initiative de l'autorité contractante ou sur proposition du titulaire, dès que son contenu, en particulier la définition des informations à protéger, nécessite une révision ou lorsque des anomalies apparaissent pendant l'exécution des travaux. Le plan contractuel de sécurité modifié doit être transmis aux destinataires figurant sur le plan initial.

¹²⁷ Par historique, il faut entendre l'ensemble des éléments de chaque contrat permettant de suivre les travaux classifiés s'y reportant. Les délais précisés ci-dessus courent pour chaque contrat à compter de la date de signature par l'autorité contractante de la FICPCS correspondante.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.8**

La fin d'exécution des travaux couverts par un plan contractuel de sécurité est matérialisée par une fiche de clôture du plan contractuel de sécurité et suit les dispositions de l'article 4.4.3.2 de l'IGI 1300.

La FICPCS permet d'enregistrer la fin d'exécution des travaux couverts par le plan contractuel de sécurité et de préciser la destination des informations et supports classifiés détenus par le titulaire pour les contrats impliquant la détention d'informations et supports classifiés. Si le titulaire demande à conserver des informations et supports classifiés, il joint l'inventaire des informations et supports classifiés qu'il a besoin de conserver, en motivant sa demande. Cette demande doit être approuvée par l'autorité contractante. Il précise la durée de conservation de ces informations et supports classifiés. Si nécessaire, cet inventaire peut être complété d'un inventaire des supports d'informations ou de niveau *Diffusion Restreinte* et sensibles que le titulaire a besoin de conserver. Lorsqu'une personne morale conserve des informations et supports classifiés après la clôture d'un plan contractuel de sécurité, elle doit faire l'objet d'une décision d'habilitation valide et d'un suivi par un service enquêteur, quand bien même cette personne morale ne serait titulaire d'aucun autre contrat générant des éléments couverts par le secret de la défense nationale.

La FICPCS est établie par le titulaire du contrat et adressée à l'autorité contractante dans un délai maximum d'un mois à compter de la fin des travaux classifiés. Le contrat peut comporter une clause liant le paiement pour solde à la fourniture de la FICPCS ou des pénalités en cas de retard.

Dans le cas d'un contrat de sous-traitance, la FICPCS doit recevoir l'accord du primo-contractant (émetteur du plan contractuel de sécurité à clore), avant d'être transmise à l'autorité contractante pour décision.

L'OS de l'autorité contractante :

- retourne au titulaire la FICPCS datée et signée en mentionnant son accord ou son refus quant à la conservation des informations et supports classifiés par le titulaire en spécifiant une durée. En cas de refus, il précise si les informations et supports classifiés figurant dans l'inventaire précité doivent lui être retournés ou être détruits par le titulaire ;
- communique simultanément la FICPCS au service enquêteur.

Le plan contractuel de sécurité d'un contrat ayant généré un ou plusieurs sous-contrats ne peut être clôturé qu'après la clôture des plans contractuels de sécurité relatifs aux sous-contrats.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.9****CAS D'UNE PERSONNE MORALE ETRANGÈRE CANDIDATE À LA
PASSATION D'UN CONTRAT IMPLIQUANT L'ACCÈS OU LA
DÉTENTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS****Références :**

- IGI 1300 – 4.4.1.4.f et 6.9
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles

Points clés

- L'article L.2353-1 du code de la commande publique exclut de la passation de marchés de défense ou de sécurité les opérateurs économiques d'Etats qui ne sont pas membres de l'Union européenne.
- Une personne morale étrangère peut candidater à un contrat impliquant l'accès ou la détention d'informations et supports classifiés sous plusieurs conditions précises qui sont vérifiées par l'autorité contractante, en liaison avec l'autorité d'habilitation.
- Les contrats impliquant l'accès ou la détention d'informations et supports classifiés portant la mention *Spécial France* ne sont pas ouverts aux candidatures de personnes morales de droit étranger.

La candidature d'une personne morale étrangère à la passation d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés nécessite que soient remplies les conditions préalables suivantes :

- il doit exister entre la France et le pays de cette personne morale un accord de sécurité définissant les principes de protection des informations et supports classifiés et les équivalences entre les niveaux d'habilitation français et ceux de ce pays (cf. fiche 9.2). Cet accord de sécurité doit couvrir le domaine concerné par le projet de contrat ;
- la communication d'informations et supports classifiés (cf. fiche 7.8) à une personne morale étrangère est subordonnée à l'autorisation écrite préalable de l'organisme à l'origine de ces informations et supports classifiés. Il appartient au prescripteur technique d'obtenir cette autorisation ;
- la personne morale étrangère et son personnel amené à avoir accès aux informations et supports classifiés doivent disposer des habilitations appropriées. La vérification de ces habilitations, auprès de l'autorité compétente de l'État dont la personne morale relève, est faite par l'autorité nationale de sécurité (cf. fiche 9.1) sur demande de l'officier de sécurité de l'autorité contractante. Si la personne morale étrangère et son personnel ne sont pas habilités au niveau approprié, une demande d'habilitation peut être formulée auprès de l'autorité étrangère compétente, *via* l'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente, si l'accord de sécurité entre le pays de cette personne morale et la France le prévoit.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.9**

Si une personne morale étrangère présente sa candidature, l'autorité contractante en informe l'autorité d'habilitation qui engage immédiatement les actions nécessaires, telles que la vérification de l'habilitation de la personne morale ou le déclenchement de la procédure d'habilitation, auprès de l'autorité de sécurité compétente dont relève la personne morale *via* l'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente.

La lettre d'invitation à participer à une consultation de tout projet de contrat impliquant l'accès ou la détention des informations portant la mention *Spécial France* ne s'adresse qu'à des personnes morales de nationalité française¹²⁸.

L'autorité nationale de sécurité ou, le cas échéant, l'autorité de sécurité déléguée compétente, peut demander à l'autorité compétente de l'État dont le candidat relève, de vérifier la conformité des locaux et installations ainsi que l'homologation des systèmes numériques susceptibles d'être utilisés, les procédures industrielles et administratives qui seront suivies, les modalités de gestion de l'information et des matériels (notamment articles contrôlés de la sécurité des systèmes d'information) ou la situation du personnel susceptible d'être employé pour l'exécution du marché.

Dans le cas d'un GME conjoint avec mandataire solidaire ou non nécessitant l'accès ou la détention d'informations ou supports portant la mention *Spécial France*, les cotraitants peuvent être des personnes morales étrangères, dans la mesure où leurs obligations contractuelles ne nécessitent pas l'accès à ces documents.

Le mandataire est reponsable de la protection des informations et supports portant la mention *Spécial France* et veille à ce que seul les cotraitants de droit français puissent y avoir accès, dans la limite du besoin d'en connaître.

Dans le cas d'un GME solidaire, nécessitant l'accès ou la détention d'informations ou supports portant la mention *Spécial France*, l'ensemble des cotraitants doivent être des personnes morales de droit français.

Dans tous les cas, le mandataire doit être de droit français.

¹²⁸ La nationalité d'une personne morale de droit privé est définie selon le pays d'implantation de son siège social.

TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES MORALES DANS LE CADRE DES CONTRATS

4.10

HABILITATION INITIALE DE LA PERSONNE MORALE

Référence :

- IGI 1300 – 4.4.1.4

Points clés

- Sauf exception¹²⁹, la procédure d'habilitation des personnes physiques employées par la personne morale est conditionnée par l'habilitation préalable de la personne morale.
- La durée de validité d'un avis de sécurité pour une habilitation personne morale est de cinq ans pour le niveau *Très Secret* et de sept ans pour le niveau *Secret*.

La personne morale doit disposer d'une habilitation en cours de validité et être titulaire du contrat ou être en phase pré contractuelle pour être autorisée à engager la procédure d'habilitation de ses salariés (cf. fiche 3.2), sous réserve de justifier pour chacune de ces personnes du besoin d'en connaître.

La procédure d'habilitation initiale obéit à la chronologie suivante :

- détermination du besoin d'habilitation (accès ou détention, niveau et nature) ;
- constitution du dossier d'habilitation de la personne morale ;
- enquête du service enquêteur qui émet un avis de sécurité adressé à l'autorité d'habilitation ;
- décision prise par l'autorité d'habilitation donnant lieu à l'habilitation ou non de la personne morale.



1. Détermination du besoin d'habilitation

L'habilitation d'une personne morale est motivée par la nécessité pour son personnel de détenir ou d'avoir accès à des informations et supports classifiés. L'exactitude et la précision des renseignements fournis dans la demande d'habilitation de la personne morale doivent faire l'objet d'un soin tout particulier. Le besoin d'habilitation d'une personne morale est émis par l'autorité contractante ou par la personne morale qui

¹²⁹ Il existe des habilitations personne physique sans qu'il soit nécessaire que la personne morale soit habilitée préalablement.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.10**

sous-contracte des prestations dont l'exécution nécessite, pour le sous-contractant, l'accès ou la détention d'informations et supports classifiés.

Toute demande sans besoin avéré d'en connaître est à proscrire.

2. Constitution du dossier d'habilitation

Le dossier d'habilitation est constitué des pièces listées à l'annexe 20 de l'IGI 1300.

Dans le cadre de la passation d'un contrat de la commande publique, le dossier d'habilitation est remis directement par le candidat à l'autorité contractante qui le retransmet à l'autorité d'habilitation. S'il est incomplet, l'autorité d'habilitation en avertit l'autorité contractante qui peut informer le candidat de la liste des pièces manquantes ou non conformes et de la date limite de fourniture de ces pièces.

3. Avis de sécurité

Dès lors que le dossier de demande d'habilitation est complet, l'autorité d'habilitation le transmet au service enquêteur qui l'instruit et fait connaître à l'autorité d'habilitation ses conclusions sous forme de deux avis de sécurité, l'un concernant la personne morale, l'autre l'un de ses représentants légaux.

Les avis de sécurité sont émis pour le niveau demandé et transmis uniquement à l'autorité d'habilitation.

S'agissant de la personne morale, les conclusions de l'avis de sécurité sont de trois types :

- avis sans objection, lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ;
- avis restrictif, lorsque la personne morale présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels elle aurait accès que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;
- avis défavorable, lorsque des informations précises font apparaître que la personne morale présente des vulnérabilités faisant peser sur le secret de la défense nationale des risques tels qu'aucune mesure de sécurité ne permet de les maîtriser.

S'agissant de l'habilitation du représentant légal de la personne morale, il convient de se référer à la fiche 3.3 de la présente instruction.

Les avis de sécurité sont émis pour un niveau donné d'habilitation. L'avis sans objection est valable pour le niveau précisé ainsi que le(s) niveau(x) inférieur(s).

Les avis restrictifs ou défavorables sont assortis d'une fiche confidentielle indiquant les motifs de l'avis. Cette fiche peut être classifiée en fonction des motifs de vulnérabilité identifiés. Ces motifs ne peuvent être portés qu'à la connaissance de l'autorité d'habilitation. Ne pouvant être reproduite, la fiche confidentielle est retournée ou détruite après communication et sans délai au service enquêteur.

L'autorité d'habilitation peut, en tant que de besoin, demander à nouveau communication des éléments qu'elle contient :

- lorsqu'elle est chargée de mettre en garde l'autorité contractante ;

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.10**

- en cas d'évolution de la situation de la personne morale ;
- à l'occasion de l'instruction d'une nouvelle demande d'habilitation la concernant ;
- pour l'instruction des recours gracieux ou contentieux dont la décision qu'elle a prise sur la base de l'avis de sécurité du service enquêteur peut faire l'objet.

La durée de validité d'un avis de sécurité est fixée au maximum à :

- cinq ans pour le niveau *Très Secret* ;
- sept ans pour le niveau *Secret*.

Un avis de sécurité peut être révisé à tout moment.

4. Décision d'habilitation**a. Procédure normale**

L'autorité d'habilitation prend sa décision après avoir pris connaissance des avis de sécurité. L'autorité d'habilitation n'est pas liée par cet avis, qui n'est qu'un des éléments parmi les actes préparatoires à sa décision. Conformément à l'article 4.4.1.1.a de l'IGI 1300, la décision d'habilitation du représentant légal de la personne morale est concomitante de la décision d'habilitation de cette même personne morale. Ces deux décisions doivent être prises au même niveau. L'autorité d'habilitation notifie sa décision à la personne morale, à l'adresse du siège social et en informe le service enquêteur. La décision prise par l'autorité d'habilitation vaut pour l'ensemble des autorités contractantes du ministère de la défense ainsi que celles agissant au profit du CEA/DAM, y compris pour les marchés duaux, en dehors de la DGSE.

Lorsque l'autorité d'habilitation considère que la personne morale ou son représentant légal présente des risques tels que la sécurité des informations et supports classifiés ne peut être garantie, elle refuse l'habilitation. Le contrat envisagé ne peut donc être attribué à la personne morale en question.

La décision de refus d'habilitation n'est pas motivée¹³⁰.

b. Procédure d'urgence

Lorsque l'avis de sécurité n'est pas émis à la date demandée, l'autorité d'habilitation peut prendre une décision d'habilitation provisoire au vu des éléments en sa possession (procédure d'urgence). Elle est d'une durée maximale de six mois. Une nouvelle décision est prise à la réception de l'avis de sécurité.

5. Domaine de validité de la décision d'habilitation

La décision d'habilitation précise le domaine de validité pour lequel elle est accordée.

Le domaine de validité concerne :

- le niveau maximum de classification des informations et supports classifiés qui peuvent être détenus par la personne morale habilitée ou communiqués au personnel habilité de cette dernière ;

¹³⁰ Article L.211-2 du code des relations entre le public et l'administration.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.10**

- les éventuelles restrictions décidées par l'autorité d'habilitation, par exemple une habilitation valable pour un programme, pour un type de contrat, pour un ou plusieurs contrats explicitement mentionnés, etc. Ces restrictions sont dispensées de motivation.

6. Identification des établissements

Lorsque le titulaire du contrat fait effectuer des travaux classifiés par des personnes relevant de plusieurs établissements, tous doivent faire l'objet d'une identification.

Cette identification doit s'effectuer lors de la transmission du dossier d'identification d'un établissement par l'autorité d'habilitation au service enquêteur. La personne morale fournit un dossier d'identification constitué des pièces suivantes :

- extrait en cours de validité du registre du commerce et des sociétés (modèle L *bis*) ;
- notice individuelle de sécurité (annexe 7 de l'IGI 1300) et lettre de proposition de l'officier de sécurité d'établissement pressenti.

L'autorité contractante annexe au dossier le plan contractuel de sécurité ou le projet du plan contractuel de sécurité.

Pour les établissements déjà identifiés, la personne morale fournit le code de sécurité économique (code SE) de l'établissement concerné.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.11****GESTION ET FIN DE L'HABILITATION DE LA PERSONNE MORALE****Référence :**

- IGI 1300 – 4.4.3.1

Points clés

- La durée de validité d'une décision d'habilitation de la personne morale ne peut excéder la durée de validité des avis de sécurité.
- Une attestation d'habilitation est fournie par la personne morale qui postule à un nouveau contrat impliquant l'accès ou la détention d'informations et supports classifiés.

1. Durée de validité d'une décision d'habilitation

La décision d'habilitation comporte une date de fin de validité qui peut être antérieure à celle qui figure sur l'avis de sécurité. Elle ne peut excéder la durée de validité de l'avis de sécurité.

La décision demeure valable pour toute autre consultation d'une autorité contractante du périmètre de l'autorité d'habilitation, à l'occasion d'un autre contrat, dans les limites de date et de domaine de validité de cette habilitation et sauf changement dans la situation de fait ou de droit de la personne morale considérée.

La durée de validité d'une décision d'habilitation est au maximum de :

- cinq ans pour le niveau *Très Secret* ;
- sept ans pour le niveau *Secret*.

2. Attestation d'habilitation

Le titulaire d'un contrat détenteur d'une décision d'habilitation en cours de validité peut faire valoir cette qualité auprès d'une autorité d'habilitation, d'une autorité contractante ou d'un officier de sécurité en produisant une attestation sollicitée auprès de l'autorité ayant prononcé l'habilitation.

Aucune communication d'informations à des tiers, à caractère commercial, publicitaire, technique ou scientifique, par des titulaires de contrats impliquant l'accès ou la détention d'informations et supports classifiés ne doit contenir de mention se référant à ces contrats, sauf autorisation expresse de l'autorité contractante. Une telle clause doit obligatoirement figurer dans le contrat.

3. Renouvellement d'habilitation

Sous réserve que le titulaire du contrat ait toujours besoin d'être habilité, en particulier si la décision d'habilitation arrive à expiration en cours de contrat, le renouvellement de son habilitation doit être demandé, par son représentant légal ou son OS, dans l'année ou six mois au plus tard avant la date d'expiration de la décision d'habilitation en vigueur. Si cette disposition est respectée, la décision d'habilitation initiale reste valable pendant les douze mois qui suivent son expiration.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.11**

La procédure est à engager directement auprès de l'autorité d'habilitation, qui s'assure auprès de l'autorité contractante du besoin de renouvellement.

Les pièces constitutives du dossier de renouvellement d'habilitation à fournir par le titulaire du contrat sont identiques à celles du dossier initial (cf. fiche 4.10).

Le dossier de renouvellement d'habilitation est transmis par l'autorité d'habilitation au service enquêteur¹³¹, qui émet un nouvel avis de sécurité.

4. Réexamen d'habilitation

L'habilitation d'une personne morale peut faire l'objet d'un réexamen, à l'initiative du service enquêteur, de l'autorité d'habilitation ou de la personne morale concernée. C'est le cas en particulier lorsque :

- la situation de la personne morale a subi des modifications de fait ou de droit (en particulier les fusions, acquisitions, rachat ou cession d'activité de la personne morale) : l'autorité d'habilitation apprécie si cette modification est de nature à remettre en cause sa décision d'habilitation et demande alors un nouvel avis ;
- le titulaire du contrat ne respecte pas ses obligations réglementaires et contractuelles relatives à la protection du secret.

Lorsque le domaine de validité de la décision d'habilitation n'est pas approprié à un nouveau besoin, une nouvelle demande doit être effectuée. Dans son rôle de conseil de la direction de la personne morale, il est nécessaire que l'officier de sécurité de celle-ci anticipe ces opérations et prenne l'avis du service enquêteur et de l'autorité d'habilitation. Cet avis peut porter sur l'éventuel maintien des habilitations ou sur les modalités de transfert des plans contractuels de sécurité liées aux contrats et permettra ainsi une mise en œuvre efficace du volet sécurité dans l'évolution de la personne morale.

Tout changement doit être porté sans délai à la connaissance de l'autorité d'habilitation et de l'autorité contractante par l'officier de sécurité ou le représentant légal de la personne morale. Sur la base des éléments recueillis et éventuellement d'un nouvel avis de sécurité, l'autorité d'habilitation peut prononcer une nouvelle décision d'habilitation.

5. Abrogation de l'habilitation de la personne morale

L'abrogation de l'habilitation de la personne morale titulaire d'un contrat peut intervenir à tout moment si elle ne remplit plus les conditions nécessaires à sa délivrance. Cette abrogation est prise par l'autorité d'habilitation, si besoin après avis du service enquêteur. Les autorités contractantes concernées sont informées par l'autorité d'habilitation.

L'abrogation de la décision d'habilitation peut entraîner la résiliation du contrat. Les conséquences d'une telle décision devant être examinées au cas par cas.

¹³¹ Via SOPHIA pour la DRSD.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.12****GESTION DES SOUS-CONTRACTANTS¹³² DANS LES CONTRATS
AVEC ACCÈS OU DÉTENTION D'INFORMATIONS ET SUPPORTS
CLASSIFIÉS****Référence :**

- IGI 1300 – 4.4.2.2.c

Points clés

- Le plan contractuel de sécurité établi entre l'autorité contractante et le primo-contractant intègre obligatoirement les informations nécessaires au suivi des prestations classifiées au sein des sous-contractants.
- L'entité primo-contractante formule la demande d'habilitation pour les personnes morales parties à un sous-contrat auprès de l'autorité contractante.
- Le contrat entre le primo-contractant et le sous-contractant doit comprendre un plan contractuel de sécurité spécifique à la nature des prestations classifiées de l'entité concernée.

Lorsqu'une personne morale titulaire d'un contrat impliquant l'accès ou la détention d'informations et supports classifiés conclut un sous-contrat amenant, notamment, à sous-traiter une partie des prestations classifiées dont elle a la charge, elle prend l'appellation de « primo-contractant » vis-à-vis de son sous-contractant.

Tout contrat nécessitant l'accès ou la détention d'informations et supports classifiés donnant lieu à au moins un sous-contrat nécessitant lui-même un accès à des informations et supports classifiés doit intégrer dans son plan contractuel de sécurité la liste des sous-contractants concernés, les travaux réalisés et leurs dates prévisionnelles de début et de fin d'exécution ainsi que les informations et supports classifiés dont la connaissance est nécessaire à leur réalisation.

1. Habilitation du sous-contractant

- Si le sous-contractant pressenti n'est pas habilité pour le domaine concerné ou au niveau requis pour les travaux concernés : il incombe à l'officier de sécurité du primo-contractant de transmettre la demande d'habilitation (fiche justificative du besoin d'habilitation) auprès de l'autorité d'habilitation.
- Si le sous-contractant est habilité : il transmet son dossier d'habilitation au primo-contractant.

L'habilitation du sous-contractant s'accompagne chez lui de la mise en place d'une structure de sécurité adaptée aux travaux classifiés qu'il doit exécuter.

¹³² Les sous-contractants (article L.2393-1 à L.2393-9, R.2393-2 à R.2393-23 du code de la commande publique) peuvent être des sous-traitants (art. L.2393-1, L.2393-10 à L.2393-14, R.2393-24 à R.2393-40 du code de la commande publique) ou des opérateurs ayant la qualité de fournisseurs ou de prestataires de services qui ne sont pas réalisés spécialement pour répondre aux besoins de l'acheteur (article L.2393-1 et L.2393-15, R.2393-41 à R.2393-44 du code de la commande publique).

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.12****2. Aptitude des locaux et homologation des systèmes numériques du sous-contractant**

La vérification des aptitudes et le début d'exécution des travaux classifiés au titre d'un sous-contrat impliquant la détention d'informations et supports classifiés suivent les dispositions des fiches 5.7 et 6.3 de la présente instruction. Le service enquêteur délivre ses avis d'aptitude à la personne morale liée par contrat au ministère, titulaire du sous-contrat et informe le primo-contractant, l'autorité contractante et l'autorité d'habilitation. Les systèmes numériques du sous-contractant sont homologués au niveau requis pour l'exécution du contrat avant de pouvoir héberger des informations.

3. Le plan contractuel de sécurité associé au sous-contrat

Le sous-contrat comporte obligatoirement un plan contractuel de sécurité dont l'établissement et la validation suivent les dispositions de la fiche 4.8. Le sous-contrat comporte les clauses de protection du secret.

La simple copie de la totalité du plan contractuel de sécurité du primo-contractant dans le projet du plan contractuel de sécurité du sous-contrat est proscrite car elle alourdit inutilement le plan contractuel de sécurité lié au sous-contrat et peut conduire à des compromissions (besoin d'en connaître). Seules les rubriques concernant la participation effective du futur titulaire du sous-contrat doivent être retenues et développées selon les modalités d'exécution des travaux qui lui sont confiés.

Le plan contractuel de sécurité d'un contrat ayant généré un ou plusieurs sous-contrats ne peut être clôturé qu'après clôture de tous les plans contractuels de sécurité des sous-contrats (cf. fiche 4.8).

Traitants ou sous-contractants non déclarés ou non identifiés

Si, en cours d'exécution, l'autorité contractante est informée de l'existence d'un sous-traitant ou d'un sous-contractant non déclaré, elle doit mettre en demeure le primo-contractant de régulariser la situation. Une fois la déclaration effectuée, les demandes d'habilitation sont transmises à l'autorité d'habilitation par le primo-contractant.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.13****CONTRÔLES DES PERSONNES MORALES PAR LES AUTORITÉS
CONTRACTANTES, LES AUTORITÉS D'HABILITATION, L'AUTORITÉ
DE SÉCURITÉ DÉLÉGUÉE ET LE SERVICE ENQUÊTEUR****Références :**

- Code de la défense – articles R.2311-9-1, D.3126-6 et D.3126-7
- IGI 1300 – 2.3.3
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Les personnes morales habilitées sont soumises au contrôle externe de l'autorité contractante, de l'autorité d'habilitation, de l'autorité de sécurité déléguée et du service enquêteur.
- Ces contrôles permettent au ministère de la défense de vérifier la bonne application des plans contractuels de sécurité et des mesures de protection du secret par les personnes morales sous contrat avec lui.

Les contrôles¹³³ menés par les autorités contractantes et d'habilitation, du service enquêteur, voire de l'autorité de sécurité déléguée dans le cadre de contrats internationaux, ont pour objet la vérification de la conformité des dispositifs de protection mise en place en application :

- de la réglementation relative à la protection du secret (dont la présente instruction ministérielle) et aux articles contrôlés de la sécurité des systèmes d'information ;
- des dispositions du plan contractuel de sécurité.

Mesurant l'écart entre la réglementation en vigueur et son application par la personne morale, ils permettent de disposer d'un état des lieux global du niveau de protection, actualisé et objectivé, destiné à évaluer la capacité d'un titulaire ou d'un sous-contractant à répondre aux exigences du contrat dans les domaines de la conservation des informations sensibles ou *Diffusion Restreinte*, des articles contrôlés de la sécurité des systèmes d'information et des informations et supports classifiés.

1. Périmètre

Les contrôles sont effectués dans les établissements des personnes morales titulaires de contrats impliquant l'accès ou la détention d'informations et supports classifiés, d'articles contrôlés de la sécurité des systèmes d'information ou d'informations sensibles ou *Diffusion Restreinte*, comme des sous-traitants ou des sous-contractants, participant ou ayant participé à des travaux avec détention.

¹³³ La notion de contrôle recouvre les contrôles, inspections ou audits précisés dans la fiche 2.9.

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.13**

Ces contrôles ont pour but de s'assurer de la mise en place de mesures de protection conformes à la réglementation et d'en vérifier l'application, lorsque des informations et supports classifiés, articles contrôlés de la sécurité des systèmes d'information, informations sensibles ou *Diffusion Restreinte* sont détenus dans les établissements du contractant.

Ils portent sur les moyens humains, matériels, technologiques, organisationnels et d'infrastructures déployés par la personne morale pour assurer la protection, l'intégrité, la manipulation, la conservation et la traçabilité des informations et supports classifiés, des articles contrôlés de la sécurité des systèmes d'information et des informations *Diffusion Restreinte* ou sensibles objets du contrat.

2. Périodicité

Les contrôles sont réalisés, dans la mesure du possible :

- en début de contrat avant la mise à disposition des informations sensibles ou *Diffusion Restreinte*, des articles contrôlés de la sécurité des systèmes d'information et des informations et supports classifiés dans les locaux du contractant et sur les systèmes numériques devant abriter des informations *Diffusion Restreinte*, sensibles ou des informations et supports classifiés ;
- à l'issue de manquement ou d'incident de sécurité impliquant le contractant ;
- en cours d'exécution à l'initiative des autorités contractantes de référence, d'habilitation et de sécurité déléguée ;
- à la clôture du contrat.

Toute personne morale liée au ministère de la défense par un contrat impliquant l'accès ou la détention d'informations et supports classifiés peut ainsi faire l'objet d'une inspection du service enquêteur ou d'un audit par l'autorité d'habilitation, l'autorité de sécurité déléguée ou l'autorité contractante (cf. fiche 2.9).

Le délai raisonnable entre deux inspections est fixé à cinq ans lorsqu'il y a détention d'informations et supports classifiés.

Le ministre, notamment à travers le service du haut fonctionnaire correspondant de défense et de sécurité (DPID) en lien avec le directeur du service enquêteur ainsi que les autorités d'habilitation, contractantes et de sécurité déléguée peuvent déclencher une inspection ou un audit de manière inopinée. L'autorité contractante peut solliciter une inspection auprès du service enquêteur.

3. Compte-rendu et suite donnée aux contrôles, aux audits et aux inspections

À l'issue du contrôle, d'un audit ou d'une inspection, les autorités contractantes et d'habilitation ou le service enquêteur rédigent un compte-rendu de l'état des lieux objectif du niveau de protection de la personne morale et des éventuelles vulnérabilités constatées.

Lorsqu'elles révèlent des insuffisances, les conclusions des contrôles, audits ou inspections donnent lieu à des actions correctives. Dans ce cas, un contrôle ultérieur permet d'en vérifier l'efficacité.

À réception du compte-rendu, la personne morale contrôlée dispose de six mois pour rendre compte à l'autorité contractante, à l'autorité d'habilitation, à l'autorité de

**TITRE 4 : MESURES DE SECURITE APPLICABLES AUX PERSONNES
MORALES DANS LE CADRE DES CONTRATS****4.13**

sécurité déléguée et au service enquêteur des mesures correctives apportées ou engagées sur son site.

Le refus de procéder à tout ou partie de ces actions correctives peut entraîner :

- sans préjudice des sanctions pénales et civiles, les conséquences dues au non-respect des dispositions acceptées contractuellement lors de l'engagement initial, comme la résiliation du contrat avec dédommagement de l'autorité contractante ;
- la révision temporaire ou définitive des aptitudes physique et informatique de l'établissement pour non-respect des prescriptions de sécurité et pour inobservation de la réglementation relative à la protection du secret de la défense nationale. Cette disposition peut entraîner la remise en cause du contrat et l'application de pénalités ;
- l'abrogation des décisions d'habilitation de la personne morale et des personnes physiques. Cette décision d'abrogation n'entraîne pas la résiliation de fait du contrat mais impose à l'autorité contractante d'identifier ou non si la poursuite de l'exécution du contrat est possible.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

INTRODUCTION : NORMES DE PROTECTION PHYSIQUE ET LOGIQUE APPLICABLES AUX INFORMATIONS ET SUPPORTS CLASSIFIÉS

Références :

- IGI 1300 – 5.2 et annexes 30 et 31

Points clés

- Les mesures de protection appliquées aux lieux abritant¹³⁴ des informations et supports classifiés ou dans lesquels ces derniers sont communiqués ou manipulés sans y être conservés, ont pour objet d'éviter toute perte, dégradation ou compromission. Elles comprennent des moyens organisationnels, humains, techniques et logiques dissociés ou combinés en fonction du niveau de classification et des menaces identifiées.
- La protection physique des informations et supports classifiés implique également de sécuriser l'accès à des locaux techniques qui peuvent être distants (énergie, moyens de communication par exemple) et assure une protection contre les menaces extérieures et environnementales (dispositifs contre les incendies, les dégâts des eaux, les risques liés à l'alimentation électrique et tout autre risque environnemental identifié).
- Lorsque les circonstances imposent la détention d'informations et supports classifiés mais ne permettent pas la mise en place des moyens habituels de protection, des mesures compensatoires sont prises afin de conserver le même niveau de protection. Ces mesures de substitution doivent procéder d'une analyse précise des risques, effectuée par l'autorité responsable du site concerné (ou l'autorité qualifiée en sécurité des systèmes d'information pour les mesures logiques) et suivre l'avis du service enquêteur compétent¹³⁵.
- Un ensemble de recommandations est formulé en complément, en [annexe 13](#).

1. Méthode et effet final recherché en matière de protection physique des informations et supports classifiés

L'identification des moyens à mettre en œuvre pour garantir la protection physique des informations et supports classifiés, déclinée dans la politique de protection du secret, s'appuie sur une analyse de risques.

Cette analyse de risques est réalisée par l'organisme abritant des informations et supports classifiés. Elle procède d'une réflexion sur les menaces qui pèsent sur l'activité,

¹³⁴ Les lieux dans lesquels sont communiqués ou manipulés des informations et supports classifiés, sans y être conservés, ne sont pas des lieux abritant, au sens de l'IGI 1300.

¹³⁵ La DRSD pour le cas général, la DGSE pour ses besoins propres.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

les installations, les personnes, le matériel et les informations de l'organisme¹³⁶. Elle couvre l'ensemble de la sûreté/sécurité du site. Dans le cadre de la protection des informations et supports classifiés, l'analyse de risques débute par l'identification des éléments de contexte¹³⁷ qui influent sur le niveau de risque. Elle se poursuit par la construction de scénarios d'atteintes aux informations et supports classifiés commises par des auteurs internes ou externes et l'identification de leurs modes d'action directs (vol, destruction, sabotage, etc.) ou indirects (ingénierie sociale, etc.).

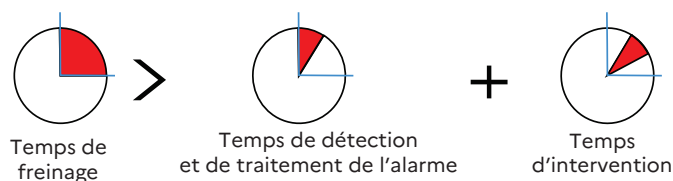
Conformément au principe de défense en profondeur (barrières successives), la protection globale des informations et supports classifiés s'obtient par une combinaison de moyens techniques (contrôle d'accès, détection d'intrusion et vidéo-surveillance, clôtures, etc.), humains (adaptation contractuelle¹³⁸, engagement de responsabilité, recrutements spécifiques etc.), organisationnels (sensibilisation, règlement intérieur, consigne etc.) et logiques (en présence d'un système numérique classifié). Seule une combinaison judicieuse de ces quatre facteurs permet d'obtenir une réponse adaptée aux risques.

Les mesures physiques mises en œuvre visent à dissuader, détecter et freiner l'intrusion afin de permettre l'intervention. Elles s'inscrivent dans la profondeur en superposant différentes couches de protection, appelées également barrières (périphériques¹³⁹, périmétriques¹⁴⁰ et intérieures), qui s'appuient essentiellement sur :

- l'emprise, le site, le bâtiment ;
- le local (ou un groupe de locaux regroupés en zone) ;
- le meuble dans lequel sont conservés les informations et supports classifiés ;
- le système numérique contenant les informations et supports classifiés.

Le choix du dispositif global de protection par le responsable d'organisme, sur les conseils de l'officier de sécurité, doit permettre d'atteindre l'équation de sûreté, définie comme suit (T pour « temps ») :

$$T \text{ freinage} > T \text{ de détection et de traitement de l'alarme} + T \text{ intervention}$$



Le temps de freinage équivaut au temps mis par l'intrus pour franchir les différentes barrières de protection placées entre la détection et les actifs ou la zone à protéger. Il

¹³⁶ Guide d'analyse de risques réalisé par la DPID/DRSD, publié en octobre 2023, disponible sur le site de la DPID.

¹³⁷ Facteurs géographiques, sociologiques, économiques, géopolitiques, etc.

¹³⁸ Cela peut correspondre à des avenants de contrat de travail, des protocoles avec des universités pour les doctorants par exemple.

¹³⁹ Partie extérieure de l'emprise (ou site) à protéger, souvent matérialisée par la limite de propriété.

¹⁴⁰ Zone située entre la partie extérieure de la propriété et les locaux à protéger, souvent matérialisée par l'enveloppe du bâtiment.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

est matérialisé par la présence de moyens de freinage en nombre et en nature suffisants.

Le temps de détection et de traitement de l'alarme correspond au délai existant entre l'alarme émise par le premier moyen de détection d'intrusion et sa prise en compte effective par l'élément chargé d'intervenir dans les meilleurs délais. Il inclut les délais de levée de doute et de transmission. À titre d'exemple :

- dans le cas d'une alarme fondée sur une détection électronique, T de détection et de traitement de l'alarme = 0 + validation de l'information (levée de doute effectuée) + délais de transmission et prise en compte effective par le poste pouvant exécuter l'intervention immédiatement, 24h/24 et 7/7 ;
- dans le cas de rondes en l'absence d'alarme ou de surveillance à distance, T de détection et de traitement de l'alarme = intervalle entre les rondes + validation de l'information (levée de doute effectuée) + délais de transmission et prise en compte effective par le poste pouvant exécuter l'intervention immédiatement, 24h/24 et 7j/7.

Le temps de détection comprend le temps mis par le moyen de détection pour transmettre l'alerte vers l'élément d'intervention (téléphonie automatique ou manuelle, radio portative, sirène, etc.). La nécessité de lever le doute sur l'effectivité de l'intrusion pour réaliser une intervention efficace (nature, volume, localisation et attitude des intrus) vient augmenter la valeur de ce paramètre.

Le temps d'intervention est le temps mis par l'élément chargé de l'intervention (interne ou externe¹⁴¹ à l'emprise du lieu abritant) pour se trouver au cœur de la zone d'action. Il tient compte de la distance à parcourir pour se rendre sur place, du temps moyen constaté pour la parcourir et de la disponibilité moyenne de l'élément d'intervention. En cas de doute, le temps majorant est retenu.

2. Recommandations pour atteindre l'équation de sûreté

Les tableaux qui suivent formulent des recommandations cohérentes et homogènes sur les combinaisons possibles de moyens techniques, humains et organisationnels¹⁴², le cas échéant, logiques, permettant d'atteindre l'équation de sûreté, en réponse aux scénarios de menaces mis en évidence par l'analyse de risques.

En cas d'impossibilité, des solutions équivalentes doivent être mises en œuvre pour atteindre cet objectif global.

Le niveau de protection des informations et supports classifiés repose sur la mise en place de trois barrières réparties en classes de résistance (de la moins à la plus résistante).

¹⁴¹ L'élément d'intervention peut être externe et s'entend au sens des forces de sécurité intérieure, d'une société de gardiennage, etc.

¹⁴² Les moyens organisationnels incluent les dispositifs juridiques.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

1. Classes du bâtiment ou de l'emprise ou du site

Classe	Description
4	<p>Emprise (ou site) dont le périmètre est délimité physiquement, disposant d'une protection mécanique (clôture dont le franchissement n'est pas possible sans facilitateur¹⁴³) et dont tous les points d'accès sont contrôlés¹⁴⁴ et assortis d'un dispositif de verrouillage mécanique ou électromécanique¹⁴⁵.</p> <p style="text-align: center;"><u>ou</u></p> <p>Bâtiment dont les ouvrants accessibles¹⁴⁶ sont, dans la mesure du possible, rendus discrets¹⁴⁷ et systématiquement dotés d'une protection mécanique (barreaux par exemple) et dont tous les points d'accès sont contrôlés¹⁴⁸ et assortis d'un dispositif de verrouillage mécanique ou électromagnétique¹⁴⁹.</p> <p><i>Nota</i> : Bien que la présence de moyens de détection d'intrusion ne soit pas imposée à ce niveau, l'existence d'un tel dispositif permet d'augmenter significativement le niveau de sûreté et peut donc être prise en compte dans l'équation de sûreté.</p>
3	<p>Enceinte¹⁵⁰ de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès conforme à l'annexe 31 de l'IGI 1300, par identification¹⁵¹ en périmétrie pour les flux piétons et véhicules ; + personnel de surveillance¹⁵² présent en permanence, effectuant des rondes dans l'enceinte et ses sous-ensembles ; + élément d'intervention extérieur mobilisable sur alarme du personnel de surveillance. <p style="text-align: center;"><u>ou</u></p> <p>Enceinte¹⁵³ de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès conforme à l'annexe 31 de l'IGI 1300, par identification en périmétrie pour les flux piétons et véhicules ; + moyen de détection d'ouverture sur les ouvrants accessibles¹⁵⁴ et les points d'accès relié à une centrale d'intrusion ; + système de vidéosurveillance/détection sur les zones sensibles permettant une levée de doute ; <p>Ces dispositifs techniques de détection-alarme sont reliés à un élément d'intervention extérieur.</p>

¹⁴³ Pierre servant de marchepieds, perche, canne, escalade, etc.

¹⁴⁴ Au moyen d'une solution ou d'un dispositif de contrôle d'accès adapté.

¹⁴⁵ Ce dispositif assure un verrouillage permanent en cas de coupure de courant.

¹⁴⁶ Étant entendu que l'accessibilité s'apprécie au regard d'un seuil minimal de 40 cm x 11 cm.

¹⁴⁷ Moyen permanent interdisant les vues de l'extérieur (par exemple : film opacifiant).

¹⁴⁸ Au moyen d'une solution ou d'un dispositif de contrôle d'accès adapté.

¹⁴⁹ Ce dispositif assure un verrouillage permanent en cas de coupure du courant.

¹⁵⁰ Emprise (ou site) ou bâtiment.

¹⁵¹ L'identification s'appuie sur un des facteurs suivants :

- ce que l'on sait (un code) ;
- ce que l'on a (un badge, une clé) ;
- ce que l'on est (comparaison biométrique ; cela inclut également ce que l'on sait faire).

¹⁵² Par exemple, agent privé de sécurité, gardien-veilleur, garde.

¹⁵³ Emprise (ou site) ou bâtiment.

¹⁵⁴ Depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc. Un accès est un trou dans une paroi permettant le passage (estimé à 40cm*11cm).

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

Classe	Description
2	<p>Les exigences de sécurité à remplir pour une emprise de classe 2 peuvent être atteintes par une combinaison de moyens humains et techniques, s'ajoutant aux éléments de la classe 4 et s'articulant de la façon suivante :</p> <p>Enceinte de classe 4 :</p> <ul style="list-style-type: none"> + contrôle d'accès conforme à l'annexe 31 de l'IGI 1300, par identification en périmétrie pour les flux piétons et véhicules ; + personnel de surveillance présent en permanence, effectuant des rondes dans l'enceinte et ses sous-ensembles ; + ensemble de télé-sécurité (télésurveillance + intervention) ; + dispositifs techniques de détection-alarme dont : <ul style="list-style-type: none"> - un moyen de détection volumétrique sur les lieux de passage permettant d'accéder aux lieux abritant des informations et supports classifiés (ISC) ; - traçabilité des entrées et sorties au niveau du bâtiment (ou d'un groupement de bâtiments) hébergeant les lieux abritant des informations et supports classifiés.
1	<p>Enceinte de classe 2 :</p> <ul style="list-style-type: none"> + présence à l'extérieur du local d'un système de vidéosurveillance des accès ; + moyen de détection d'intrusion placé sur tous les points d'accès des lieux abritant les informations et supports classifiés ; + présence permanente sur site d'un élément humain d'intervention.

2. Classes du local

Si l'emprise ne présente pas de dispositif de détection-alarme, un dispositif de ce type doit être installé au niveau du local.

Les parois des locaux (plafonds, sols et murs) ainsi que les ouvrants (portes, fenêtres, etc.)¹⁵⁵, leurs serrures et leurs sùretés doivent présenter une résistance mécanique suffisante et homogène pour retarder l'intrusion et permettre la mise en œuvre des moyens d'intervention.

Toutes les serrures des portes des locaux sont équipées d'un dispositif de verrouillage mécanique, électromagnétique ou motorisé comme dispositif principal¹⁵⁶.

Les fabricants de sùreté à clef justifient que leurs produits possèdent :

- une technologie qui s'oppose aux techniques d'ouverture à l'aide d'outils manuels ;

¹⁵⁵ Les dispositifs électromécaniques ou électromagnétiques de fermeture des ouvrants ne peuvent pas à eux seuls garantir l'intégrité des accès aux bâtiments ou aux emprises. Ils doivent obligatoirement être complétés par des systèmes mécaniques de verrouillage mis en service en dehors des périodes d'occupation des bâtiments.

¹⁵⁶ Le cas échéant, tout dispositif électronique est complété par un dispositif de verrouillage mécanique, électromagnétique ou motorisé. Les clés de secours sont conservées selon les dispositions du 7.2.3 de l'IGI 1300.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

- une conception qui complique l'usage de moyens d'ouverture fine (outils spécifiques dits « de crochetage »).

La fourniture et la reproduction de la clef ne doivent être possibles qu'après l'authentification d'une personne désignée auprès du fournisseur. La présence d'une carte dite de propriété ne peut pas, à elle seule, suffire comme moyen de protection contre la copie.

Classe	Description
d	Local avec bloc-porte à serrure mono point et baies fermées (fenêtres, évacuateur de fumées, blocs de climatiseur, etc.).
c	Local avec : <ul style="list-style-type: none"> ○ bloc-porte (métallique ou en bois plein ou matériau équivalent) à serrure mécanique multipoints ; ○ sûreté à clé présentant un temps de résistance suffisant¹⁵⁷ ; ○ contrôle d'accès par identification ; ○ fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.). <p>À l'intérieur des lieux abritant les informations et supports classifiés :</p> <ul style="list-style-type: none"> ○ moyen de détection volumétrique double technologie relié à une centrale d'intrusion ; <p style="text-align: center;"><u>ou</u></p> <ul style="list-style-type: none"> ○ moyen de détection d'intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.).
b	Local avec : <ul style="list-style-type: none"> ○ bloc-porte renforcé équipé d'un système anti-dégondage à serrure mécanique multipoints avec détecteur ; ○ sûreté à clef présentant un temps de résistance suffisant¹⁵⁸ ; ○ fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.) ; ○ contrôle d'accès par authentification avec traçabilité des entrées et sorties. <p>À l'intérieur des lieux abritant les informations et supports classifiés :</p> <ul style="list-style-type: none"> ○ moyen de détection intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.) ; ○ moyen de détection volumétrique double technologie relié à une centrale d'intrusion ; ○ système permettant la levée de doute en dehors des heures de service (vidéosurveillance, par ex.).
a	Chambre forte ¹⁵⁹ dont le bloc-porte est au minimum équipé des systèmes de sécurité des armoires fortes de classe B.

¹⁵⁷ En référence à la norme NF-EN 1627 ou équivalente, la classe de résistance CR3 (= 5 minutes) peut servir de référence. L'outillage est précisé.

¹⁵⁸ En référence à la norme NF-EN 1627 ou équivalente, la classe de résistance CR5 (= 15 minutes) peut servir de référence. L'outillage est précisé.

¹⁵⁹ Le local répond aux exigences de la norme NF-EN 1143-1 ou équivalente.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

3. Classes du meuble

Les meubles de sécurité destinés à la conservation des informations et supports classifiés ne peuvent pas être ouverts frauduleusement sans effraction : toute tentative d'ouverture illégitime laisse des traces visibles détectables par l'utilisateur. Ils sont dotés par défaut de serrures à combinaison mécanique conformes à la norme EN1300 niveau B (ou équivalente) minimum.

Les meubles prévus pour protéger des équipements électroniques en fonctionnement sont naturellement pourvus d'ouïes de ventilation. En raison de l'accès visuel sur le contenu offert par leur présence, ces meubles ne doivent pas contenir de supports à lecture directe.

Classe	Description
C	Armoire forte à structure métallique d'au moins 2 millimètres d'épaisseur, munie d'une serrure mécanique à combinaison silencieuse et à manœuvre discrète. Les battants possèdent un système d'accrochage du côté du pivot interdisant le démontage des portes en cas de sectionnement des gonds, lorsque le meuble est condamné. Les pênes, inaccessibles de l'extérieur, ne doivent pas pouvoir être démontés.
B	<p>Armoire forte de structure identique à celle de classe C :</p> <ul style="list-style-type: none"> + renforcement de la structure de la zone située entre la face avant de la porte et les organes essentiels dont la présence peut être vérifiée visuellement par démontage du foncet de porte (face intérieure de la porte) ; + dispositif délateur, à déclenchement mécanique et thermique, bloquant définitivement les mécanismes d'ouverture en cas de tentative d'ouverture illégitime ; + plombage du foncet de porte (face intérieure de la porte) permettant de détecter aisément un démontage ; + système à clef interdisant l'accès au dispositif de changement de la combinaison pour les modèles mécaniques ; + système d'asservissement, interdisant la sortie des pênes de la porte principale lorsque l'autre battant n'est pas fermé, s'il ne s'agit pas d'un meuble à porte unique ; + dispositif qui interdit aux pênes de la porte principale, une fois sortis, de se rétracter à moins que la combinaison soit à nouveau composée ; + compteur d'ouverture non falsifiable et non réutilisable, sans dispositif de remise à zéro et protégé par le foncet ; + une serrure mécanique à combinaison silencieuse et à manœuvre discrète est à recommander. L'emploi d'une serrure électronique, conforme à la norme EN1300 niveau B au minimum, disposant d'un dispositif de composition discret et assurant la traçabilité des combinaisons, peut être autorisé s'il est justifié ; <p>Le meuble équipé d'une serrure à combinaison électronique comporte une serrure mécanique à clef facilement permutable en supplément. Cette clef est prisonnière de la serrure tant que le pêne de la serrure à combinaison et ceux du meuble ne sont pas sortis portes fermées ;</p>

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

Classe	Description
	<p>+ système de tringlerie métallique en acier assurant sur la porte principale une répartition géographique de plusieurs pènes horizontaux et verticaux. Si une poignée actionne ce système, elle possède un point de rupture pour éviter un effort trop conséquent sur la tringlerie.</p> <p>Les portes sont dépourvues de toute plaque de propreté et de tout enjoliveur.</p>
A	<p>Coffre-fort blindé sur toutes ses faces, d'un poids minimum à vide de 500 kg ou, à défaut, fixé au mur, au sol ou sur une plaque métallique dont la plus petite dimension est supérieure à la plus grande dimension des issues du local.</p> <p>Ce meuble comporte tous les systèmes de sécurité de la classe B :</p> <p>+ une ou plusieurs serrures pouvant s'adapter à un nouveau jeu de clefs (serrures mécaniques dites à clef facilement permutables) ;</p> <p>+ au moins une serrure dont la clef reste prisonnière du mécanisme tant que le pêne de la combinaison et les pènes du meuble ne sont pas sortis porte fermée.</p> <p>La marque et le numéro de série du meuble sont estampillés de façon apparente et inaltérable, à l'extérieur de celui-ci, sur le corps et sur toutes les portes du meuble ; le numéro de série et l'année de fabrication de chaque serrure figurent sur celles-ci.</p>

4. Classes des postes utilisateurs classifiés

Il est possible de déroger aux mesures de protection logiques prévues ci-dessous en mettant en œuvre des mesures de protection compensatoires, sous réserve de leur validation formelle par l'autorité d'homologation pour le niveau *Secret* ou, pour le niveau *Très Secret*, par l'autorité qualifiée de la sécurité des systèmes d'information.

Description	Classe γ de base	Classe β renforcé	Classe α fort
Intégrité physique des éléments constitutifs du système numérique	Scellés génériques de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu des scellés Contrôle ponctuel de l'intégrité des scellés par l'utilisateur.	Protection de la classe γ + Contrôle annuel de l'intégrité des scellés.	Dispositif de détection d'ouverture de l'équipement ou scellés numérotés de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu ces scellés Contrôle semestriel de l'intégrité des scellés.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

Description	Classe γ de base	Classe β renforcé	Classe α fort
Confidentialité des données lorsque le terminal ¹⁶⁰ n'est pas en fonctionnement	Chiffrement des données utilisateur par un logiciel agréé pour la protection des informations portant la mention <i>Diffusion Restreinte</i> ou Stockage à distance des données sur l'infrastructure d'hébergement du système numérique ou Mémoire de masse extractible ou équipement mobile stockable dans un meuble de classe adaptée à la classification des données en clair	Chiffrement intégral du disque par un logiciel agréé pour la protection des informations portant la mention <i>Diffusion Restreinte</i> ou Stockage à distance des données sur l'infrastructure d'hébergement du système numérique ou Mémoire de masse extractible ou équipement mobile stockable dans un meuble de classe adaptée à la classification des données en clair	Protection de la classe β
Sécurité du contrôle d'accès de l'utilisateur	Mot de passe avec politique de sécurité des mots de passe conforme à la politique de sécurité de l'organisme	Dispositif d'authentification forte ¹⁶¹ , par exemple basée sur une infrastructure de gestion de clefs (IGC) conforme au RGS** ¹⁶² - homologuée par l'organisme	Dispositif d'authentification forte, par exemple basée sur une IGC qualifiée au moins RGS**.
Accès aux dispositifs d'import - export du poste utilisateur	Réservé aux utilisateurs authentifiés sur le terminal + supports amovibles préalablement « enrôlés » sur le système et	Protection de la classe γ	Réservé aux utilisateurs assurant une fonction d'enregistrement des documents classifiés ou de gestion des échanges

¹⁶⁰ Le terminal s'entend comme le poste utilisateur fixe, nomade ou mobile, qui permet l'accès et le traitement des informations classifiées lorsqu'il est en fonctionnement.

¹⁶¹ Le non-respect de cette exigence doit être justifié dans le dossier d'homologation.

¹⁶² Le référentiel général de sécurité (RGS) publié par l'ANSSI est le cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Son niveau est déterminé par le nombre d'étoiles (une, deux ou trois étoiles).

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

Description	Classe γ de base autorisés pour cet utilisateur	Classe β renforcé	Classe α fort
Contrôle des équipements connectés au réseau	Désactivation des services non utilisés (conformité)	Protection de la classe γ + Authentification des équipements au réseau	Protection de la classe β
Cloisonnement et filtrage	Cloisonnement par fonction homogène au sein du système numérique (cloisonnement des réseaux locaux-LANs- par population)	Cloisonnement entre les utilisateurs d'une même population, exemple P-VLAN.	Cloisonnement par le chiffre pour chaque poste utilisateur (tunnel dédié vers les services)
Capacité à restreindre la visualisation des IC par un tiers.	Disposition des terminaux par rapport aux ouvertures du local (portes, fenêtres, vasistas, hublots, etc.) et protection des vis-à-vis	Protection de la classe γ	Protection de la classe β

3. Tableaux de combinaison des classes

L'objectif final est d'égaliser ou de surpasser le temps de freinage tel que défini au point 1 pour obtenir un niveau de sécurité minimal pour les informations et supports classifiés.

La détermination de ce niveau est réalisée en trois temps :

- la classification des barrières (emprise (ou site) ou bâtiment, local, meuble ou moyen logique) ;
- les moyens de détection d'intrusion ou de freinage qui leur sont associés ;
- la vérification de la validité de la combinaison des classes des barrières en fonction du niveau de classification des informations et supports classifiés.

Dans le cas où le niveau minimal de sécurité ne peut être atteint, il faut faire évoluer la classe d'une ou des barrières pour atteindre ce niveau.

a. Protection des informations et supports classifiés

La protection des informations et supports classifiés est assurée par trois barrières physiques successives au niveau de l'emprise (ou site) ou du bâtiment, du local et du meuble.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

Les tableaux 1 et 2 définissent, pour chaque niveau de classification, la classe minimale du meuble en fonction des classes de protection du bâtiment et du local.

Tableau 1 : niveau *Secret*

CLASSE DU BÂTIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	C	C	C	C
2	C	C	C	C
3	C	C	C	B
4	C	C	B	interdit

Si des informations et supports classifiés au niveau *Secret*, hors systèmes d'information classifiés, ne peuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils sont alors conservés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise (ou site) ou le bâtiment est au minimum de classe 3. Un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur ;
- le local est au minimum de classe c avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment¹⁶³.

S'agissant des systèmes d'informations classifiés au niveau *Secret*, les mesures de sécurité sont conformes à celles définies au tableau 3.

Tableau 2 : niveau *Très Secret*

CLASSE DU BÂTIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	C	C	interdit	interdit
2	C	C	interdit	interdit
3	C	C	interdit	interdit
4	interdit	interdit	interdit	interdit

Si des informations et supports classifiés au niveau *Très Secret*, hors systèmes d'information classifiés, ne peuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils sont alors conservés dans un local renforcé correspondant aux caractéristiques suivantes :

¹⁶³ Les détecteurs sont généralement raccordés à une centrale locale placée dans le local ou la zone, sans qu'aucun élément (câblage par exemple) ne sorte de la zone à protéger. C'est la liaison entre les centrales locale et générale qui peut sortir de la zone, sous réserve qu'elle soit chiffrée. C'est en cela que le système est indépendant. Il ne s'agit donc pas obligatoirement de déployer deux systèmes d'information de détection d'intrusion.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

- l’emprise (ou site) ou le bâtiment est au minimum de classe 2. Un contrôle permanent de la zone est organisé en s’appuyant sur un dispositif de détection-alarme relié à un élément d’intervention extérieur ;
- le local est au minimum de classe b avec un dispositif de détection-alarme indépendant de ceux de l’emprise/bâtiment¹⁶⁶.

S’agissant des systèmes d’informations classifiés au niveau *Très Secret*, les mesures de sécurité sont conformes à celles définies au tableau 4.

b. Protection des systèmes d’information classifiés

La protection des systèmes d’information classifiés est assurée par la combinaison de deux barrières physiques et d’une barrière logique.

Les tableaux 3 et 4 définissent, pour chaque niveau de classification, la classe minimale de la protection logique en fonction des classes de protection physique de l’emprise (ou site) ou du bâtiment et du local. La lettre grecque désigne la classe du système numérique classifié.

Tableau 3 : niveau *Secret*

CLASSE DU BÂTIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	Υ	Υ	β	β
2	Υ	Υ	β	β
3	Υ	Υ	β	α
4	Υ	Υ	α	interdit

Tableau 4 : niveau *Très Secret*

CLASSE DU BÂTIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	β	β	interdit	interdit
2	β	β	interdit	interdit
3	β	β	interdit	interdit
4	interdit	interdit	interdit	interdit

Dans l’hypothèse où les barrières physiques sont assurées par le local et un meuble adapté, sans considération du niveau de protection du bâtiment, le tableau 5 définit, pour le seul niveau de classification *Secret*, la classe minimale de protection logique.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS
CLASSIFIÉS

5.1

Tableau 5 : niveau Secret

Cas particulier : classe minimale du système numérique pour le niveau Secret

Classe du meuble	Classe du local			
	a	b	c	d
A	γ	γ	β	α
B	γ	γ	β	α
C	γ	β	α	α

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.1****ZONE PROTÉGÉE****Références :**

Code de la défense – article R.2362-1 et articles D.2362-2 à D.2362-4
Code pénal – articles 413-7 et R.413-8 et R.413-1 à R.413-5
IGI 1300 – 5.3.1.1

Points clés

- Une zone protégée confère une protection juridique renforcée à l'emprise ou au site ou au local.
- Elle est conseillée pour les lieux abritant des informations et supports classifiés au niveau *Secret* et obligatoire au niveau *Très Secret*.
- Le statut de zone protégée permet d'avoir recours au contrôle primaire au titre du contrôle d'accès.

1. Définition, dispositions juridiques et réglementaires

La zone protégée est un terrain ou un local clos, auquel l'accès est soumis à autorisation afin de protéger les installations, les matériels, le secret des recherches, des études ou des fabrications ou les informations et supports classifiés qui s'y trouvent. Ses limites et son interdiction de libre accès sont rendues visibles afin de ne pas être franchies par inadvertance.

La désignation en tant que zone protégée assure une protection juridique à des infrastructures sensibles. Les articles 413-7 et 413-8¹⁶⁴ du code pénal définissent les peines applicables en cas de pénétration ou de tentative de pénétration dans une zone protégée.

Tout bien meuble (aéronef, navire, véhicule) ou immeuble situé à l'intérieur d'une zone protégée bénéficie de la protection juridique de celle-ci.

2. Création d'une zone protégée**a. Règle de classement en zone protégée**

Le classement des locaux et installations relevant du ministère de la défense en zone protégée est :

¹⁶⁴ Article 413-7 du code pénal : « est puni de six mois d'emprisonnement et de 7 500 € d'amende le fait, dans les services, établissements ou entreprises, publics ou privés, intéressant la défense nationale, de s'introduire sans autorisation, à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications. Un décret en Conseil d'État détermine, d'une part, les conditions dans lesquelles il est procédé à la délimitation des locaux et terrains visés à l'alinéa précédent et, d'autre part, les conditions dans lesquelles les autorisations d'y pénétrer peuvent être délivrées ».
Article 413-8 du code pénal : « la tentative des délits prévus aux articles 413-2 et 413-5 à 413-7 est punie des mêmes peines ».

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS 5.1

- obligatoire dès que ces locaux ou emprises conservent des informations et supports classifiés d'un niveau supérieur au *Secret* (ou mention équivalente) ; ces informations et supports classifiés sont conservés en zone réservée (voir fiche 5.2), elle-même incluse ou confondue avec une zone protégée ;
- à privilégier chaque fois que possible pour assurer la protection des installations, du matériel, du secret des recherches, études ou fabrications et des informations et supports classifiés au niveau *Secret*. Le besoin de protection doit alors être justifié.

Le classement en zone protégée de la totalité d'une emprise est à privilégier lorsqu'elle contient plusieurs locaux ou zones de ce type.

Pour les points d'importance vitale, il est, par ailleurs, conseillé, chaque fois que cela est possible, de créer une zone protégée ayant les mêmes limites que le site.

Toutefois, il est important d'étudier chaque dossier au regard des différentes réglementations afin de concilier le meilleur rapport coût-efficacité, la mise en œuvre de mesures de protection adaptées et le besoin de protéger les informations et supports classifiés ainsi que les locaux abritant des matériels sensibles.

b. Autorité de décision

Par délégation du ministre de la défense, les autorités mentionnées à l'article D.2362-2 du code de la défense sont compétentes pour déterminer le besoin de protection des zones protégées.

Dans la limite de leur compétence respective, les autorités mentionnées aux articles D.2362-2 et D.2362-3 du code de la défense sont compétentes pour fixer l'implantation et les limites des zones protégées.

c. Procédure de création

Pour permettre aux autorités de signer l'arrêté portant création de zone protégée, le responsable d'organisme adresse à l'autorité compétente au sens des dispositions des articles D.2362-2 à D.2362-4 du code de la défense qui émet la décision de création, une demande¹⁶⁵ qui comprend au moins :

- la justification du besoin de protection ;
- un plan du site sur lequel figure avec précision le contour envisagé de la zone protégée envisagée ;
- l'avis de l'organisme enquêteur compétent sur l'herméticité effective de la zone et sur les conditions matérielles et organisationnelles du contrôle de ses accès ;
- une copie du précédent arrêté portant création de la zone protégée dans le cas d'une demande relative à sa modification.

¹⁶⁵ Le modèle de dossier de création de zone protégée est accessible sur le site Armement (<https://armement.defense.gouv.fr/securite-et-habilitation/habilitation-des-personnes-morales-et-physiques/zone-protegee>).

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS 5.1

L'arrêté de création n'est pas classifié. Il est adressé au responsable de l'organisme dont l'emprise ou le local est concerné, avec copie au ministre de l'intérieur et aux préfets territorialement compétents (article R.413-4 du code pénal modifié¹⁶⁶).

Une copie de cet arrêté est également adressée, par l'organisme responsable du site, à l'organisme enquêteur compétent.

Pour assurer son opposabilité, l'arrêté doit faire l'objet d'une publication¹⁶⁷. Sa date de publication doit apparaître sur les pancartes de manière visible, sur le périmètre défini de la zone protégée.

3. Dispositif de protection

a. Généralités

Le classement en zone protégée confère à l'installation une protection juridique mais ne correspond pas à un niveau de protection physique.

Néanmoins, la zone protégée doit être matérialisée de telle sorte qu'elle ne puisse pas faire l'objet d'une pénétration par inadvertance. En pratique, cela se caractérise par la mise en œuvre de dispositifs et de mesures de protection physique (murs, barrières, obstacles, etc.).

La pénétration sans autorisation dans une zone protégée constitue un délit ; elle autorise l'application de l'article 73 du code de procédure pénale :

1. l'appréhension d'un intrus ;
2. la présentation à un officier de police judiciaire.

Le classement en zone protégée n'a pas d'incidence sur les règles d'emploi de la force et d'usage des armes sur le territoire national prévues aux articles L.2338-3 du code de la défense et L.435-1 du code de la sécurité intérieure (1^o à 4^o pour la protection des installations militaires).

b. Matérialisation de la zone protégée

L'article R.413-4 du code pénal fait obligation de rendre apparentes les limites des zones protégées. Des panneaux faisant référence à l'article 413-7 du code pénal doivent être placés au niveau de tous les accès, principaux et secondaires, de l'installation considérée de façon à matérialiser avec évidence et sans ambiguïté le classement de l'emprise ou du bâtiment en zone protégée. Par ailleurs, des panneaux identiques doivent être placés aux endroits appropriés et en nombre suffisant pour interdire le franchissement par inadvertance.

¹⁶⁶ Article R.413-4 : « L'arrêté portant création d'une zone protégée est notifié au chef du service, de l'établissement ou de l'entreprise. Celui-ci prend alors, sous le contrôle de l'autorité qui a déterminé le besoin de protection, toutes dispositions pour rendre apparentes les limites de la zone et les mesures d'interdiction dont elle est l'objet. Un exemplaire de l'arrêté est adressé, pour leur information et éventuellement aux fins d'application des dispositions qui les concernent, au ministre de l'intérieur et aux préfets territorialement compétents. ».

¹⁶⁷ Conformément à l'article L.221-2 du code des relations entre le public et l'administration.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS
CLASSIFIÉS****5.1**

Les panneaux d'interdiction revêtent la forme suivante :



La taille de la police d'écriture :

- « zone protégée » = 60 mm de hauteur ;
- le reste du texte = 30 mm de hauteur.

Les lettres sont de couleur noire peinte sur un fond blanc.

Les panneaux doivent respecter ces dimensions dès lors que de nouveaux panneaux doivent être confectionnés. Ils doivent être conçus dans un matériau résistant aux intempéries.

c. Contrôle des accès

Afin qu'aucune pénétration à l'intérieur d'une zone protégée ne puisse survenir par inadvertance, tous ses accès doivent être contrôlés en permanence. Ce contrôle d'accès se fait par identification, quels que soient les moyens techniques ou humains, mis en place.

Le système numérique permettant, le cas échéant, de contrôler les accès en zone protégée, homologué par l'autorité d'emploi, met en œuvre des mécanismes d'authentification et d'intégrité garantissant l'accès à ce système par les seules personnes autorisées. À défaut d'un tel système, un registre physique répondant aux mêmes objectifs, accessible aux seules personnes assurant des responsabilités dans le contrôle d'accès (agents de sécurité, officier de sécurité, etc.) et dûment identifiées dans l'organisation, est utilisé pour les visiteurs pénétrant en zone protégée.

Tout accédant à une zone protégée doit faire l'objet d'un contrôle primaire. Seul le responsable de la zone protégée peut autoriser une dérogation à cette règle si et seulement si l'accédant est accompagné en permanence (cf. fiche 3.9).

L'autorisation de pénétrer au sein d'une zone protégée dans laquelle se trouve un lieu abritant des informations et supports classifiés est donnée par le responsable

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.1

d'organisme, selon les directives et sous le contrôle de l'autorité ayant déterminé le besoin de protection.

En revanche, pour protéger des recherches, études ou fabrications qui doivent être tenues secrètes dans l'intérêt de la défense nationale, aux termes de l'article R.413-5-1, il est créé une zone à régime restrictif, après autorisation de création de la zone à régime restrictif délivrée par l'autorité¹⁶⁸ qui a déterminé le besoin de protection.

Dans tous les cas, l'autorisation est délivrée par écrit et peut être retirée à tout moment dans les mêmes formes (article R.413-5 du code pénal).

Sous contrôle du ministre, le responsable d'organisme a toute latitude pour définir les mesures générales et particulières propres à assurer le contrôle d'accès le mieux adapté aux conditions locales. Il est habilité à prendre toutes les mesures particulières de restriction d'accès qu'il juge nécessaires au regard des circonstances ou de la spécificité de la zone protégée.

¹⁶⁸ Une autorisation écrite transmise par mail est valable.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.2****ZONE RÉSERVÉE****Références :**

- Code pénal – articles 413-7, 413-8 et articles R.413-1 à R.413-5
- IGI 1300 – 5.3.1.2, annexe 32
- Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 sur la protection contre les signaux parasites compromettants
- Note n° 3273/ARM/CAB/CM1-C.HFD/DR du 13 juin 2019 relative à l'utilisation de la carte d'identité multi-services (CIMS) pour le contrôle d'accès

Points clés

- Une zone réservée est obligatoire pour la protection physique des informations et supports classifiés de niveau *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale.
- La zone réservée doit être incluse dans une zone protégée.

1. Principes

Une zone réservée est obligatoire pour la protection physique des informations et supports classifiés de niveau *Très Secret* quelle que soit leur nature (national, OTAN, UE), y compris ceux faisant l'objet d'une classification spéciale. Elle a pour but de renforcer le niveau de protection physique, électronique et organisationnel en cohérence avec le niveau de classification des informations et supports, y compris les systèmes d'information, conservés à l'intérieur.

La zone réservée n'apportant pas de protection juridique spécifique, elle doit donc être incluse dans une zone protégée telle que définie à la fiche 5.1. de la présente instruction.

Les impossibilités techniques empêchant la création d'une zone protégée doivent être justifiées, notamment pour les informations et supports classifiés détenus sur un moyen mobile (bateau, avion, véhicule roulant, etc.) ou à l'étranger (cf. Fiche 5.3 et Titre 10).

2. Dispositions administratives de création d'une zone réservée

Il appartient au responsable d'organisme qui élabore, traite, reçoit ou détient des informations et supports classifiés de niveau *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale, de créer une zone réservée.

Le traitement ou la conservation d'informations et supports classifiés dans ces locaux ne peut intervenir qu'après avis technique d'aptitude physique (ATAP) et, le cas échéant, avis technique d'aptitude informatique (ATAI) conformes (cf. fiche 6.3). Ces avis sont rendus après dépôt auprès du service enquêteur d'un dossier de demande

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.2

d'aptitude pour chaque lieu abritant¹⁶⁹ (cf. fiche 5.7 et annexe 11) ou pour chaque système numérique traitant des informations et supports classifiés.

La décision de création, signée par le responsable d'organisme, doit comprendre la localisation de la zone réservée ainsi que les références de la zone protégée dans laquelle se situe la zone réservée (cf. modèle en annexe 10). Elle est transmise à l'officier de sécurité, au bureau de protection du secret et au responsable de la zone réservée.

3. Mesures de protection

L'ensemble des mesures décrites ci-après constitue le régime de protection de la zone réservée. Elles doivent être précisées dans une note signée par le responsable de la zone réservée.

a. Mesures de protection physique

Les mesures de protection de la zone réservée doivent respecter le principe de l'équation de sûreté (cf. Introduction du titre 5). À ce titre, le local érigé en zone réservée doit :

- être pourvu d'ouvertures en nombre restreint¹⁷⁰ et à la protection renforcée avec, notamment pour chaque ouvrant, y compris l'issue de secours, la présence d'un dispositif de détection intrusion ;
- disposer d'un meuble de sécurité ;
- être placé sous détection d'intrusion¹⁷¹ dès que les locaux ne sont pas occupés ;
- disposer d'un système de détection-alarme indépendant de tout autre système .

Si des systèmes d'information classifiés de niveau *Très Secret* sont utilisés dans la zone réservée, les mesures relatives aux circuits approuvés (cf. PSSI-M et fiche 6.10) et aux signaux parasites compromettants (SPC) sont à mettre en œuvre.

b. Mesures organisationnelles

Un contrôle permanent de la zone réservée doit être organisé en s'appuyant sur un dispositif de surveillance (humaine ou technique) complété par un dispositif de détection d'intrusion et de remontée d'alarme¹⁷² relié à un poste central de protection (PCP) en mesure de déclencher une intervention. En cas de besoin de discrétion, la présence de panneaux indiquant la zone réservée n'est pas obligatoire pour les locaux hébergeant des informations et supports classifiés nationaux¹⁷³.

¹⁶⁹ Les lieux dans lesquels sont communiqués ou manipulés des informations et supports classifiés sans y être conservés peuvent faire l'objet d'un avis technique d'aptitude physique, à la demande du responsable d'organisme.

¹⁷⁰ Fenêtres protégées, portes renforcées équipées de serrures de haute sécurité et issue de secours équipée d'un dispositif de détection d'intrusion.

¹⁷¹ Un système de détection volumétrique est recommandé.

¹⁷² La mise sous alarme des locaux de la zone réservée doit être indépendante des autres systèmes de détections/surveillance. Lorsque les occupants sont absents, les locaux doivent systématiquement être sous surveillance.

¹⁷³ Pour les informations et supports classifiés OTAN et UE, il convient de se référer aux dispositions particulières des instructions interministérielles 2100 et 2102.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.2

Des rondes de sécurité aux abords de la zone réservée sont régulièrement effectuées par des gardiens ayant fait l'objet d'une enquête administrative et disposant de consignes écrites précisant leur mission. En particulier, ces consignes doivent inclure les conditions pour pénétrer dans les zones réservées : nécessité de service, levée de doute, réglementation particulière, urgence avérée (cf. fiche 5.8).

Pendant les heures d'utilisation, le contrôle de la zone réservée incombe au personnel qui y est employé. Avant de quitter les lieux, celui-ci vérifie la mise en sûreté des informations et supports classifiés, la fermeture des meubles de sécurité et de tous les ouvrants puis effectue les mises sous alarme.

En dehors des heures d'utilisation, des contrôles sont organisés par l'autorité responsable ou par son bureau de protection du secret, pour vérifier :

- la fermeture des locaux, des meubles de sécurité, le fonctionnement des systèmes de détection, etc. ;
- le vidage des corbeilles à papier et l'absence de brouillon ou document préparatoire aux informations classifiées ;
- l'absence d'informations et supports classifiés hors des meubles de sécurité¹⁷⁴.

4. Contrôle d'accès

Le dispositif (organisationnel, technique ou humain) de contrôle d'accès à une zone réservée doit assurer la conservation et la protection de l'intégrité et de la disponibilité des données relatives aux accès et garantir l'authentification¹⁷⁵ de tous les accédants autorisés par le responsable de la zone.

Le contrôle d'accès en zone réservée se fait par identification avec traçabilité ou par authentification multi facteurs, c'est-à-dire par la combinaison de deux ou plus des facteurs suivants :

- ce que l'on sait (un code) ;
- ce que l'on a (un badge, une clé) ;
- ce que l'on est (comparaison biométrique, etc.).

Les données doivent être conservées conformément au droit de protection des données à caractère personnel.

Pour chaque zone réservée, une liste nominative exhaustive, avec photographie, des personnes habilitées et autorisées à pénétrer est maintenue à jour par le responsable de la zone réservée, *via* son officier de sécurité. Pour toute nouvelle autorisation d'accès ou décision de retrait d'accès, la liste actualisée est visée et paraphée par le responsable de la zone. Il est recommandé que cette liste soit affichée dans la zone réservée afin de permettre un autocontrôle par les personnes autorisées à y pénétrer.

Le personnel de soutien ne peut pénétrer dans une zone réservée que s'il a satisfait à une enquête administrative pour le renseignement et la sûreté (cf. fiche 3.9). Dans le

¹⁷⁴ À l'exception des informations et supports classifiés dont le volume et les dimensions ne permettent pas leur rangement dans un meuble de sécurité.

¹⁷⁵ La perception d'une clé d'accès en zone réservée auprès de l'officier de permanence après signature d'un registre et un code unique pour désactiver l'alarme du local constituant, pour exemple, un système d'authentification valable.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.2**

cas d'une prestation de service, une personne morale ayant passé un contrat sensible doit au préalable satisfaire à une enquête administrative. Le personnel de soutien dispose d'un laissez-passer (CIMS ou badge) permettant son identification et attestant de la décision d'accès. Il n'intervient qu'en présence de personnes habilitées de la zone réservée et lorsque les informations et supports classifiés ne lui sont plus accessibles.

Toutes les personnes n'ayant pas autorisation d'accès à la zone réservée sont considérées comme des visiteurs. Pour pénétrer dans une zone réservée, les visiteurs doivent être identifiés et enregistrés¹⁷⁶ au préalable, faire l'objet d'une décision d'accès délivrée par l'autorité responsable de la zone réservée et être munis d'un laissez passer (carte CIMS ou badge - visiteur ou temporaire - attribué nominativement au visiteur pour la durée de la visite) permettant leur identification et attestant de la décision d'accès.

Tous les visiteurs doivent être accompagnés par des personnes habilitées désignées parmi le personnel de la zone réservée, pendant toute la durée de la visite.

Seuls les visiteurs habilités au niveau requis accèdent aux informations et supports classifiés pour lesquels ils ont le besoin d'en connaître.

L'ensemble des mesures encadrant la sécurité des visites dans une zone réservée¹⁷⁷ et adaptées à la configuration de cette dernière doit être décrit dans le régime de protection de la zone réservée.

5. Cas exceptionnel de la zone réservée temporaire

Le traitement ou la conservation d'informations et supports classifiés de niveau *Très Secret* ne peut intervenir en dehors d'une zone réservée. Il peut être dérogé à cette règle de manière exceptionnelle, pour des raisons opérationnelles ou de préparation opérationnelle, et exclusivement de façon temporaire.

Il est alors créé une zone réservée temporaire, par le responsable d'organisme, qui peut, lorsque les conditions ne sont pas réunies, ne pas s'inclure à l'intérieur d'une zone protégée.

Cette zone réservée temporaire doit être soumise aux mesures de sécurité définies aux points 3 et 4 de cette fiche.

Dans le cas d'un déploiement hors du territoire national, une zone bénéficiant de mesures de protection spécifiques à une zone à accès réservé est créée (cf. titre 10).

¹⁷⁶ L'organisme doit conserver une trace de l'identité du visiteur, du motif de la visite et de la date et l'heure de la visite.

¹⁷⁷ Ces mesures doivent inclure un circuit de notoriété, s'il existe.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.3****ÉLÉMENTS CLASSIFIÉS CONSERVÉS HORS COFFRE****Références :**

- IGI 1300 – 5.2.2 et annexe 30
- Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 sur la protection contre les signaux parasites compromettants

Points clés

- Les informations et supports classifiés trop grands ou trop volumineux pour être enfermés dans des meubles de sécurité (informations et supports classifiés dits hors coffre) doivent bénéficier de mesures de protection compensatoires.
- Les informations et supports classifiés conservés hors coffre dans des moyens mobiles, hors opérations, sont soumis à des règles particulières et doivent être gardés en permanence.

1. Principes

Compte tenu de leurs dimensions, certaines informations et supports classifiés de niveaux *Secret* et *Très Secret* (comme des prototypes, des pièces usinées ou des objets, par exemple) ne peuvent être conservés dans un coffre ou dans une armoire forte alors que les dispositions réglementaires le prévoient.

Aussi, les mesures de protection doivent être adaptées pour tenir compte de l'absence de meuble de sécurité. Ces informations et supports classifiés hors-coffre sont alors conservés dans un local répondant aux normes minimales d'infrastructure définies *infra*. Leurs conditions de conservation/stockage doivent faire l'objet d'une étude au cas par cas avec le concours du service enquêteur. Dans la mesure des possibilités techniques, un dispositif de masquage des informations et supports classifiés doit être installé (par exemple : rideaux, diffusion d'une fumée opacifiante sur détection d'intrusion).

Les informations et supports classifiés conservés dans des moyens mobiles doivent être, quant à eux, gardés en permanence (cf. point 3.). Enfin, il peut exceptionnellement exister des informations et supports classifiés qui ne sont ni mobiles ni conservés dans un local. Leur protection doit être étudiée au cas par cas en liaison avec le service enquêteur.

2. Informations et supports classifiés hors-coffre de niveau *Secret*

Le local est au moins de classe c avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment et répond aux normes suivantes :

- le bâtiment ou l'emprise dans lequel il est situé est au moins de classe 3 ;
- un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.3

Classe de l'emprise / bâtiment	Classe du local			
	a	b	c	d
1	autorisé	autorisé	autorisé	interdit
2	autorisé	autorisé	autorisé	interdit
3	autorisé	autorisé	autorisé	interdit
4	interdit	interdit	interdit	interdit

3. Informations et supports classifiés hors-coffres de niveau *Très Secret*

Les informations et supports classifiés trop grands ou trop volumineux pour être enfermés dans des meubles de sécurité doivent être situés dans une zone réservée (cf. fiche 5.2) et conservés dans un local renforcé correspondant aux caractéristiques suivantes :

- l'emprise ou le bâtiment est au minimum de classe 2. Un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur ;
- le local est au minimum de classe b avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment.

Classe de l'emprise / bâtiment	Classe du local			
	a	b	c	d
1	autorisé	autorisé	interdit	interdit
2	autorisé (1)	autorisé (1)	interdit	interdit
3	interdit	interdit	interdit	interdit
4	interdit	interdit	interdit	interdit

(1) Le local zone réservée et l'emprise sont équipés de dispositifs de détection alarme indépendants.

4. Moyens mobiles du ministère de la défense

La protection des informations et supports classifiés abrités dans des moyens mobiles en opération n'est pas traitée dans la présente fiche et fait l'objet d'une directive technique particulière.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.3

Pour les mobiles (aéronefs, navires, véhicule, etc.) abritant des informations et supports classifiés situés sur leur entité de rattachement ou en déplacement en dehors de cette dernière, les modalités de protection suivantes sont à appliquer.

	En terrain militaire sur le territoire national	Hors terrain militaire sur le territoire national	Zone civile sur un territoire étranger	Zone militaire sur un territoire étranger ¹⁷⁸
Gardiennage par des agents du ministère ¹⁷⁹ ou des FSI	Autorisé (1)	Autorisé (1)	Autorisé (1)	Autorisé (1)
Gardiennage par des sociétés en contrat avec le ministère de la défense ou avec un OIV du ministère de la défense	Autorisé (1)	Autorisé (1)	Interdit (2)	Interdit (2)
Autres cas	Interdit (2)	Interdit (2)	Interdit (2)	Interdit (2)

(1) à la condition de verrouiller les accès au mobile¹⁸⁰.

(2) conservation des informations et supports classifiés sur l'homme en permanence (uniquement pour le Secret) ou à la mission de défense de l'ambassade.

La protection du secret dans les navires

Un navire à quai ou au mouillage dans son port-base sur le territoire de la République Française bénéficie du statut de zone protégée lorsqu'une telle zone a été déclarée au sein de la base navale et que le bâtiment s'y trouve.

À défaut, lorsque le navire se trouve hors d'une zone protégée, au port-base, en escale en France hors du port-base ou en escale à l'étranger, il a le statut de zone militaire tel que défini à l'article 413-5 du code pénal. Le navire de guerre bénéficie, en outre, d'immunités de législation, de juridiction et d'exécution permettant en mer comme à quai dans un port étranger, d'y interdire le libre accès.

Dans le cas d'entretien ou de maintien en condition opérationnelle :

- soit la responsabilité est transférée à l'industriel selon les modalités prévues dans le plan contractuel de sécurité ;
- soit la responsabilité n'est pas transférée à l'industriel, dès lors la sûreté à bord revient au commandant du bâtiment.

¹⁷⁸ Le gardiennage est assuré après analyse de risques au regard des accords négociés avec la nation hôte.

¹⁷⁹ Ou, pour le CEA exclusivement, des forces locales de sécurité (FLS).

¹⁸⁰ Le verrouillage des accès d'un aéronef consiste en la mise en œuvre d'un dispositif de verrouillage mécanique à clé et l'apposition de scellés de sûreté.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.3**

Un navire de guerre peut disposer de lieux abritant des éléments couverts par le secret de la défense nationale. Les informations et supports classifiés conservés dans un navire de guerre font l'objet d'un dispositif de protection destiné à les protéger contre toute menace, externe ou interne, qui pourrait remettre en cause leur disponibilité, leur intégrité, leur confidentialité et leur traçabilité et à empêcher qu'une personne non qualifiée puisse y accéder. Il s'appuie sur une analyse de risques et s'inscrit dans une logique de défense en profondeur qui repose sur des barrières successives.

La protection du secret dans les aéronefs

Un aéronef dans lequel sont conservés des informations et supports classifiés est un lieu abritant.

Au sol, les aéronefs dans lesquels sont manipulés ou conservés des informations et supports classifiés doivent obligatoirement être gardés. Sur une base aérienne, aéronavale ou au sein de l'aviation légère de l'armée de Terre, les aéronefs bénéficient des protections et des mesures associées à la zone protégée. Posés sur un terrain sommaire ou à l'étranger, les aéronefs font l'objet des mêmes mesures et protections, adaptées aux ressources disponibles. Les aéronefs qui sont embarqués à bord d'un porte-avions ou d'un bâtiment porte-hélicoptères relèvent des dispositions du paragraphe précédent (protection du secret dans les navires) dès lors qu'ils se trouvent physiquement sur le navire de guerre.

En vol, l'aéronef embarquant des informations et supports classifiés intègre des dispositifs limitatifs à base de chiffrement ainsi que des dispositifs physiques ou logiques de protection de l'information en cas d'avarie pouvant amener la perte de contrôle de l'aéronef. La perte en vol d'un aéronef transportant des informations et supports classifiés entraîne la rédaction d'un procès-verbal de perte d'informations et supports classifiés.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.4****ACTIVITÉS NÉCESSITANT L'ACCÈS À DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS EN DEHORS DE LEUR LIEU ABRITANT****Référence :**

- IGI 1300 – 5.4.3 et annexe 35

Points clés

- Le lieu dans lequel sont traités ou manipulés temporairement des informations et supports classifiés, en particulier une réunion, une conférence, une présentation de matériel, ne nécessite pas l'émission d'un avis technique d'aptitude physique (ATAP) par le service enquêteur. Ce lieu se distingue du lieu dans lequel sont communiqués ou manipulés des informations et supports classifiés sans y être conservés et pour lequel un avis technique d'aptitude physique peut être demandé par le responsable d'établissement (cf. fiche 5.0).
- Pour une réunion, tous les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont à classer au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

1. Principes

Dès lors que des informations et supports classifiés sont manipulés en dehors du lieu les abritant en temps normal (dans le cas, par exemple, d'une réunion, d'une conférence ou d'une présentation de matériel), l'organisateur applique les recommandations suivantes avant, durant et après la communication des informations et supports classifiés. Il en informe l'OS dont il dépend. Sa responsabilité pénale est, en cas de compromission, susceptible d'être engagée sur le fondement de l'article 413-10 du code pénal. Cela ne désengage cependant pas le détenteur de sa responsabilité. Le lieu dans lequel se déroule l'activité doit être sécurisé et son accès contrôlé. Il peut s'agir d'un lieu dédié au traitement des informations et supports classifiés ou d'un lieu « neutre ». Néanmoins, dans ce dernier cas, le niveau maximal de classification des informations évoquées au cours de la réunion ne doit pas dépasser les capacités de protection de la salle accueillant la réunion. Aucun avis préalable d'aptitude physique n'est cependant requis lorsque le lieu n'est pas dédié.

2. Choix du lieu pour l'activité

Le local prévu pour la séance au cours de laquelle sont manipulés des informations et supports classifiés doit répondre à des contraintes d'isolement, d'accès et de protection physique. Ainsi, il est recommandé :

- d'éviter un local donnant sur l'extérieur ;
- de privilégier un local à l'abri des écoutes indirectes, à l'écart des voies d'accès desservant le bâtiment ou les constructions voisines, sans mitoyenneté vulnérable sur les façades ;
- de ne pas indiquer la destination du local ;

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.4**

- pour le local disposer de fenêtres protégées, d'un accès unique avec une porte en bois plein ou blindée, rappel automatique et serrure de sûreté sans poignée extérieure ;
- de ne donner l'accès qu'aux personnes autorisées pour interdire toute intrusion avant la réunion ;
- d'éviter tout élément de rangement (tiroir, meuble) ou matériel qui ne soit pas utile au déroulement de l'activité.

Un contrôle des lieux est effectué sous la responsabilité de l'organisateur avant, éventuellement pendant et après l'activité.

Une attention particulière est portée aux opérations de nettoyage, d'entretien, et de réparation du local comme de ses installations annexes et des pièces mitoyennes. L'accompagnement autant que possible des personnes intervenant au titre des maintenances diverses doit impérativement être mis en œuvre afin d'éviter tout piégeage des lieux.

3. Préparation de l'activité au cours de laquelle sont manipulés des informations et supports classifiés

Dès lors que le niveau de classification, les limites et le degré de précision à apporter dans les échanges sont connus, il faut veiller à ce que l'organisateur :

- les précise sur les invitations des participants, pour permettre la désignation de personnes habilitées au niveau requis et ayant besoin d'en connaître ;
- demande aux invités d'adresser en temps utile leurs nom et fonction ainsi que leur niveau d'habilitation afin que puisse être établie la liste de toutes les personnes participant à la séance, à quelque titre que ce soit : auditeurs, conférenciers, assistants, techniciens chargés des projections ou essais, etc. ;
- rappelle, dans l'invitation, la nécessité pour les invités d'être en possession des pièces justificatives le jour de la visite (certificat de sécurité, carte d'identité).

4. Protection des informations et supports classifiés au cours de l'activité

L'organisateur :

- fait accompagner les visiteurs (participants extérieurs) ;
- s'assure de l'identité et du niveau d'habilitation de chacun des participants présents au vu des certificats de sécurité (cf. fiche 3.6) ;
- s'assure que personne ne détient d'appareils non agréés au niveau requis par l'activité permettant la captation, la réémission et l'enregistrement d'informations (téléphone mobile, ordinateur portable, objets connectés, etc.)¹⁸¹ ;
- peut interdire toute prise de note ou tout enregistrement des interventions par les auditeurs ;
- veille, en application des principes stricts de cloisonnement de l'information classifiée, en particulier pour le niveau *Très Secret*, y compris aux niveaux équivalents de l'OTAN et de l'UE et pour les informations faisant l'objet d'une classification spéciale, à ce que la communication demeure limitée à l'objet de l'activité ;

¹⁸¹ Dans le respect de la législation (article L.33-3 du code des postes et communications électroniques), l'usage de brouilleurs est possible.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.4**

- autorise les participants à quitter le local pendant les pauses, si la sécurité des informations et supports classifiés qui y sont laissés est assurée, en indiquant que chaque participant reste responsable de ses informations et supports classifiés ;
- veille à la sensibilisation des participants sur leurs obligations en matière de protection du secret de la défense¹⁸² ;
- prohibe les discussions relatives aux informations classifiées en dehors du local prévu ;
- notifie toute faille dans la sécurité à l'officier de sécurité qui en informe, le cas échéant, les participants.

5. À l'issue de l'activité

En cas de communication d'informations de niveau *Très Secret*, l'organisateur consigne, dans un procès-verbal succinct, à classifier éventuellement, les domaines d'information qui ont été exposés, les mesures prises pour en assurer la protection ainsi que la liste des participants avec mention de la justification de leur habilitation.

L'organisateur de l'activité veille à :

- la récupération et à la mise en sécurité des informations ou supports classifiés éventuellement mis à la disposition des auditeurs ;
- la destruction des supports provisoires et préparatoires.

¹⁸² Tous les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont classifiés au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.5****MATÉRIEL D'IMPRESSION, DE REPRODUCTION ET DE
DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIÉS****Références :**

- IGI 1300 – 7.2.4 et 7.5.1
- Arrêté du 20 août 2024 relatif aux normes techniques de destruction des informations et supports classifiés ou protégés
- PSSI-E – Item « Sécurisation des imprimantes et des copieurs multifonctions »

Point clé

L'impression, la reproduction et la destruction d'informations et supports classifiés doivent être effectuées sur des appareils conformes et idéalement centralisés dans un même lieu.

Les procédures de destruction, d'impression et de reproduction d'informations et supports classifiés doivent répondre à des normes strictes. Le matériel de destruction et d'impression/reproduction de la documentation classifiée de niveau *Très Secret* ou *Secret* doit être centralisé chaque fois que cela est possible.

Des signalisations indiquent sur chaque appareil le niveau maximum autorisé de sensibilité ou de classification pour la destruction, l'impression et la reproduction.

1. Matériel de destruction des informations et supports classifiés papiers

Le moyen le plus couramment utilisé pour détruire les documents papier est le déchiquetage, qui consiste à réduire le support en lambeaux (particules de moins de 10 mm² et de largeur inférieure à 1 mm).

Le matériel utilisé doit respecter la norme fixée par l'arrêté du 20 août 2024 relatif aux normes techniques de destruction des informations et supports classifiés ou protégés. Les anciens matériels utilisés avant la publication de cet arrêté restent valables dans les conditions définies par l'arrêté précité¹⁸³.

2. Matériel d'impression et de reproduction des informations et supports classifiés

De nombreux périphériques d'impression utilisent des mémoires de masse sur lesquelles sont conservées les données à traiter (comme les photocopieurs numériques, par exemple). Afin d'assurer une protection efficace des données traitées par ces équipements et des réseaux qui les mettent en œuvre, il est vivement recommandé d'adopter les mesures suivantes :

- ces appareils sont physiquement protégés pour en limiter l'emploi aux seules personnes autorisées ;

¹⁸³ Cette validité est limitée à une durée de cinq ans maximum à compter de la date de publication de l'arrêté du 20 août 2024.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.5**

- ils doivent être gérés par les directions informatiques ; une vigilance particulière s'impose de la part des responsables de la sécurité des systèmes d'information ; dès lors que des informations sensibles, *Diffusion Restreinte* ou classifiées transitent par ce type d'appareil, l'ensemble des recommandations et réglementations relatives aux systèmes d'information traitant des informations de cette nature s'applique. Si ces matériels sont connectés à un système numérique, ils sont intégrés dans le périmètre d'homologation du système numérique. Par ailleurs, il est interdit de connecter entre eux des équipements de niveau de sensibilité ou de confidentialité différents sauf dans le cas d'un dispositif agréé ou homologué à cet effet ;
- il convient de limiter le nombre de photocopieurs dédiés et autorisés à reproduire les documents sensibles, *Diffusion Restreinte* ou classifiés (une note interne fixant ce nombre est recommandée, de même que l'utilisation de pictogramme). Ces imprimantes/copieurs doivent être soit isolés, soit reliés à un réseau de même niveau de classification que l'information et support classifié reproduit. Ils prendront le même niveau de classification que les informations et supports classifiés traités ;
- lorsque cela est possible, systématiser, en lien avec les organismes en charge de l'externalisation des prestations liées aux photocopieurs, imprimantes et autres scanners, le marquage des impressions et numérisations des documents sensibles, *Diffusion Restreinte* ou classifiés (date, heure, et référence du poste d'impression), le recours à une identification par code/badge permet cette traçabilité ;
- les contrats de location et de maintenance doivent inclure des clauses relatives à la sécurité (rétention des disques durs, notamment) ;
- la télémaintenance est à proscrire pour du matériel traitant des informations et supports classifiés : aucun modem ne doit être installé dans le copieur (à défaut, il doit être physiquement désactivé) ;
- l'option fax permettant un accès vers l'extérieur est proscrite : aucune carte fax ne doit être installée dans le copieur (à défaut, elle doit être physiquement désactivée) ;
- l'utilisation par le technicien de la société de maintenance d'un moyen permettant le stockage d'informations (ordinateur portable, graveur de cédéroms, disquettes, outils de stockage USB, etc.) est interdite. Si nécessaire, l'entité utilisant le copieur doit mettre à disposition du technicien un ordinateur sans graveur de cédéroms sur lequel sont installés les logiciels et applicatifs de maintenance nécessaires ;
- avant toute opération de maintenance, le copieur doit être débranché du réseau. Il est procédé à la photocopie de quelques feuilles contenant des informations non sensibles puis à l'arrêt complet du copieur (mise hors tension quelques minutes) ;
- en cas de problème sur le disque dur du périphérique, celui-ci est soit réparé sur place, soit remplacé par un nouveau matériel ; l'élément remplacé doit être remis à l'officier de sécurité du site pour destruction ;
- le copieur ne doit pas posséder de lecteur extérieur ou de port actif (RS 232, USB, Firewire, Wifi, etc.) permettant une connexion non prévue vers l'extérieur (à défaut, il doit être physiquement désactivé) ;
- pendant toute l'opération de maintenance des copieurs du site, une personne est présente afin de contrôler l'application des règles ci-dessus ;
- ces règles doivent être affichées, de manière visible, à proximité de chaque photocopieur numérique.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.6****PROTECTION CONTRE LES COMPROMISSIONS VIA LES
ÉQUIPEMENTS ÉLECTRONIQUES****Référence :**

- IGI 1300 – 6.5.1

Points clés

- Les équipements électroniques piégés sont des vecteurs possibles pour capter des informations. Ce piégeage peut être réalisé à distance et ne nécessite pas de compétences élevées.
- Il est de la responsabilité de l'officier de sécurité de fixer les règles applicables au sein de son organisme.
- Dans les zones réservées, les équipements électroniques non fournis par l'employeur et non-homologués sont interdits.
- Un affichage doit être mis en place et permettre de s'assurer que chacun connaît les règles applicables.

1. Vulnérabilités spécifiques des équipements électroniques

Les équipements électroniques sont des vecteurs possibles pour capter ou enregistrer des informations sensibles, *Diffusion Restreinte* ou classifiées, en temps réel ou différé. Ils sont susceptibles d'être piégés, le cas échéant à l'insu de l'utilisateur, et de constituer des capteurs pour une opération d'espionnage.

Il s'agit principalement de traiter les vulnérabilités dues aux équipements électroniques munis d'un dispositif technique de captation sonore ou vidéo (ordinateurs portables, téléphones mobiles, tablettes, montres, dictaphone, écouteurs/micro sans fils, caméra, etc.) connectés à l'espace cybernétique (Internet, téléphone portable, WIFI, Bluetooth, indirectement par synchronisation ou mise à jour, etc.).

À titre d'illustration, un utilisateur peut être dupé par une application disponible sur un « store », donc a priori légitime et inoffensive, mais qui, en réalité, peut contenir du code malveillant capable de déclencher un enregistrement audio, lors de la reconnaissance d'un mot clé, du passage du téléphone en mode avion ou dans le cas d'absence de réseau mobile (positionnement en cage de faraday par exemple), l'enregistrement étant transmis dans un second temps. Les équipements professionnels, y compris ceux agréés par l'ANSSI (*Diffusion Restreinte* ou classifié), entrent dans le champ de cette menace, même si leur vulnérabilité est moindre en raison des dispositions techniques ou organisationnelles prises.

2. Définitions

Parmi les équipements électroniques, on distinguera :

- les équipements informatiques : ordinateurs portables, tablettes-PC et tablettes. Ces objets sont généralement très connectés (WiFi, Bluetooth, réseau GSM) et sont « encombrants » (ne tiennent pas dans la poche) ;
- les équipements mobiles : téléphone, smartphone. Ces objets sont connectés à des réseaux publics et sont peu encombrants (tiennent dans la poche) ;

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.6**

- les objets connectés (et assimilés) : objets munis d'un moyen de captation sonore ou vidéo et pouvant être connectés directement à un réseau public (GSM, WiFi, etc.) ou indirectement (synchronisation ou mise à jour *via* un ordinateur ou un smartphone).

Les équipements électroniques utilisés à des fins médicales sont exclus.

Pour chacun de ces types d'équipements électroniques, on distinguera la provenance et l'utilisation :

- personnelle : l'utilisateur est propriétaire et seul responsable de sa gestion ou de sa sécurisation ;
- professionnelle : l'employeur fournit un équipement dont il est propriétaire et dont il définit le niveau de sécurité et les règles d'emploi.

3. Cadre général

D'un point de vue général, il est de la responsabilité de l'officier de sécurité de définir les règles en fonction de la sensibilité des activités de son organisme¹⁸⁴. Les mesures mises en place sont proportionnées et adaptées aux spécificités et au fonctionnement de l'organisme mais aussi des emprises, des bâtiments ou des locaux qu'elle occupe.

L'officier de sécurité peut mettre en place un zonage (par exemple *via* l'identification des bâtiments ou des bureaux et salles de réunion dans lesquels sont traitées les activités sensibles) permettant d'adapter au mieux les règles à chaque zone.

Lorsque la sensibilité des activités le nécessite, l'officier de sécurité proscrit les équipements électroniques personnels et professionnels non encadrés.

Il est mis en place des dispositifs pour permettre le stockage des équipements proscrits en nombre suffisant et aux localisations nécessaires, notamment pour rendre les conditions de travail acceptables (proximité entre les salariés et leurs moyens de communication professionnels ou personnels) ou permettre l'accueil des visiteurs en toute sécurité.

Un affichage est mis en place par l'officier de sécurité pour que les règles en vigueur soient connues de tous, y compris des éventuels visiteurs.

4. Spécificités applicables pour la protection des informations et supports classifiés

En dehors des produits agréés pour traiter des informations classifiées, les équipements électroniques ne doivent en aucun cas être à moins de deux mètres d'un équipement traitant d'informations classifiées.

Dans les salles de réunion (ou autre local utilisé momentanément comme salle de réunion), les équipements électroniques non agréés (hors équipements informatiques professionnels nécessaires) sont proscrits lorsque la réunion est classifiée. Les équipements mobiles professionnels peuvent être exceptionnellement tolérés lorsqu'ils répondent à une nécessité (exemple : astreinte).

¹⁸⁴ La sensibilité d'une activité dans le cadre de la présente fiche se mesure par la sensibilité des informations traitées et le volume d'informations classifiées ou *Diffusion Restreinte* traitées.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.6**

Il est également proscrit de réaliser une visioconférence avec des moyens non classifiés dans un environnement classifié afin d'empêcher la captation vidéo d'une information classifiée visible dans l'environnement.

5. Spécificités applicables aux zones réservées

Seuls les systèmes d'informations homologués et dont l'installation est prévue dans la zone réservée peuvent y être présents.

Les objets personnels et les objets professionnels non encadrés sont interdits en zone réservée. L'officier de sécurité peut déroger à cette règle si une organisation est formalisée au sein de la zone réservée pour que les activités relevant d'un niveau *Très Secret* soient réalisées en l'absence d'objet personnels ou professionnels non encadrés.

Il revient à l'officier de sécurité de fixer les règles propres à la zone réservée en fonction de la nature des activités réalisées et de l'usage de chaque pièce. Les équipements électroniques professionnels peuvent être tolérés en zone réservée. Par exemple :

- un équipement électronique homologué pour le traitement d'informations de niveau *Très Secret* (exemple : ordinateur portable) ou un produit agréé *Très Secret* (exemple : TEOREM) peut être accepté ;
- un équipement mobile professionnel pour une personne devant rester joignable à tout moment (par exemple dans le cadre d'une astreinte) peut être toléré selon des conditions à définir ;
- un équipement informatique professionnel peut être toléré (exemple : ordinateur portable de travail) ;
- le téléphone professionnel d'une personne travaillant dans le service peut être toléré, par exemple lorsque cette personne n'est pas présente dans un local dans lequel une information classifiée *Très Secret* est en cours de traitement (c'est-à-dire audible ou visible) et qu'il peut à tout moment le déposer rapidement dans un lieu sûr en cas de besoin.

6. Autres dispositions

La localisation d'une emprise ou l'appartenance d'une personne à un organisme sont des informations qui peuvent être jugées sensibles au regard de la protection des informations. Dans ce cas, le personnel concerné est sensibilisé aux risques de géolocalisation induits par les équipements électroniques, qu'ils soient équipés d'un dispositif de géolocalisation (GPS) ou non, notamment au regard de l'usage qu'il peut en être fait, comme le suivi géolocalisé par des applications sportives. Si cette information est classifiée, une interdiction est envisagée.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.7****CONTRÔLES D'APTITUDE PHYSIQUE À LA DÉTENTION
D'INFORMATIONS ET SUPPORTS CLASSIFIÉS****Références :**

- IGI 1300 – 4.4.1.5, 5.3.3, annexes 29 à 32
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles
- IM 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées

Points clés

- La détention d'informations et supports classifiés dans un local est conditionnée à l'obtention d'un avis technique d'aptitude physique.
- L'aptitude physique est un préalable impératif à :
 - la détention d'informations et supports classifiés *Secret* en dehors d'une zone militaire,
 - la détention d'informations et supports classifiés *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale, au sein d'une zone réservée.
- L'aptitude physique est vérifiée par le service enquêteur, elle renseigne les autorités contractantes et d'habilitation sur le niveau de protection du secret atteint dans l'établissement ou l'organisme qui va exécuter les travaux classifiés.

1. Généralités

Les organismes traitant des informations et supports classifiés dans leurs locaux doivent selon les cas précisés ci-après au préalable obtenir un **avis technique d'aptitude physique** (ATAP). Ce dernier est obtenu après évaluation de l'aptitude des locaux. Le service enquêteur s'assure, notamment, que les mesures de protection physique des locaux sont cohérentes avec l'analyse de risques réalisée par l'organisme. Ces mesures doivent permettre d'entraver une atteinte à la protection du secret. Le cas échéant, il s'assure également que le système numérique de sûreté fait l'objet d'une homologation de sécurité, en suivant les règles de l'instruction interministérielle n° 901. L'officier de sécurité des systèmes d'information est responsable du suivi des systèmes de contrôle d'accès, détection d'intrusion et vidéo-surveillance de l'organisme en coordination avec l'officier de sécurité.

Enfin, dès la réception d'un avis technique d'aptitude physique, l'organisme bénéficiaire émet à la demande de l'autorité contractante ou de l'autorité d'habilitation pour les entités contractantes une attestation de conformité physique¹⁸⁵ certifiant que les mesures de protection dont bénéficie le lieu abritant sont conformes à la réglementation.

¹⁸⁵ Cf. IGI 1300, annexe 26.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.7****- Pour le niveau *Secret* :**

Les lieux abritant doivent faire l'objet d'une demande d'avis, à l'instar des établissements disposant de locaux prévus pour détenir des ISC *Secret* dans le cadre de contrats ou des lieux abritant des informations et supports classifiés *Secret* au sein du ministère de la défense situés en dehors d'une zone militaire.

Ne sont pas concernés par les demandes d'avis technique les locaux de stockage ou de traitement des informations et supports classifiés *Secret* des services ministériels ou de la direction des applications militaires du CEA (CEA/DAM) situés dans une zone militaire ou au CEA/DAM.

Pour les établissements publics sous tutelle du ministère de la défense et les organismes d'importance vitale, les demandes d'avis technique sont facultatives. Néanmoins, ces avis techniques doivent être présentés lors des inspections décidées par le service du haut fonctionnaire correspondant de défense et de sécurité.

- Pour le niveau *Très Secret* :

Les zones réservées (militaires ou non), qui abritent des informations et supports classifiés *Très Secret*, y compris ceux faisant l'objet d'une classification spéciale, doivent sans exception faire l'objet d'un avis technique d'aptitude physique.

2. Le dossier d'aptitude

Dans le cas d'un contrat ou d'une convention impliquant la détention d'informations et supports classifiés, les personnes morales candidates sont informées par l'autorité contractante des normes physiques et numériques (cf. introduction du titre 5) imposées par la détention d'informations et supports classifiés. Elles doivent satisfaire à ces normes et aux obligations induites par la détention de tels informations ou supports.

Un dossier d'aptitude doit être déposé pour chaque lieu abritant afin de solliciter un avis technique d'aptitude physique du service enquêteur.

Pour les organismes ministériels ainsi que le CEA/DAM, ce dossier comprend :

- le plan de la zone réservée et du bâtiment/emprise ;
- l'organisation et les moyens de protection et de gardiennage ;
- l'identification et la description de la protection, actuelle et envisagée, du local ou des locaux où sont conservés ou manipulés les travaux protégés. Ceci inclut l'analyse de risques du site et la liste des organismes assurant l'installation et la maintenance des systèmes numériques de sûreté concourant à la protection du local ainsi que l'analyse de risques réalisée dans le cadre de l'homologation de ces mêmes systèmes d'information.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.7**

Pour les personnes morales liées au ministère de la défense par contrat ou convention, la constitution du dossier peut prendre deux formes :

- si la personne morale envisage de réaliser les travaux classifiés dans un local n'ayant pas au préalable fait l'objet d'un avis d'aptitude « sans réserve » ou ayant fait l'objet de modifications rendant caducs les avis d'aptitude précédemment émis : un dossier d'aptitude complet doit être constitué ;
- si l'entité envisage de faire les travaux classifiés du contrat dans le local objet d'un avis technique d'aptitude physique : un dossier d'aptitude allégé comprenant la copie de l'avis d'aptitude déjà obtenu, accompagnée de l'attestation de conformité correspondante ainsi que de l'attestation de non-changement des conditions qui ont amené la délivrance de l'avis d'aptitude.

Le règlement de la consultation du marché public¹⁸⁶ indique les documents nécessaires à la constitution du dossier d'aptitude (cf. annexe 11). Ces documents sont fournis à l'autorité contractante avec l'offre dans les délais fixés dans le règlement de la consultation.

3. Evaluation et décision d'aptitude

Dès le choix de l'attributaire, l'autorité contractante informe l'autorité d'habilitation et le service enquêteur du choix de l'attributaire. L'autorité d'habilitation transmet le dossier de demande d'aptitude correspondant au service enquêteur. Lors de la notification du contrat et après étude du dossier d'aptitude, le service enquêteur et l'autorité contractante établissent un calendrier permettant de déterminer une date de début des travaux classifiés. Ce calendrier prévisionnel comprend notamment :

- une date d'évaluation initiale d'aptitude physique ;
- une date d'émission d'avis technique d'aptitude physique.

Au sein du ministère, l'organisme transmet son dossier d'aptitude au service enquêteur. Ils fixent ensemble le calendrier d'évaluation et d'émission de l'avis.

L'évaluation initiale de l'aptitude prend en compte un certain nombre de mesures de protection relatives au bâtiment et à l'emprise contenant le local, au local lui-même et au meuble de sécurité contenant les informations et supports classifiés (cf. introduction du titre 5). Elle se conclut par l'émission :

- d'un avis technique d'aptitude physique « sans objection », lorsque le niveau de sûreté répond aux exigences de protection des informations et supports classifiés, avec mesures compensatoires éventuelles. Le responsable d'organisme établit alors une attestation de conformité physique (cf. IGI 1300 – annexe 26) ;
- d'un avis technique d'aptitude physique « avec réserve », lorsque le niveau de sûreté atteint ne permet pas de répondre totalement aux exigences de protection des informations et supports classifiés. L'avis décrit les mesures compensatoires à mettre

¹⁸⁶ Le règlement est disponible sur le site Internet Armement (<https://armement.defense.gouv.fr>).

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.7**

en œuvre afin d'atteindre le seuil minimal de protection. La détention d'informations et supports classifiés peut être autorisée, sous réserve d'attester de la mise en œuvre de ces mesures compensatoires dans de brefs délais. Dans le cas contraire, le responsable d'organisme propose un plan d'action assorti d'un échéancier qui doit être accepté par le service enquêteur et l'autorité contractante. Après la mise en place de ces mesures, le responsable d'organisme transmet un certificat de mise aux normes de sécurité physique (cf. IGI 1300 – annexe 27) au service enquêteur, qui procède à un nouveau contrôle. Les mesures compensatoires sont des mesures prises localement afin de palier une vulnérabilité et de répondre à l'équation de sûreté. Elles sont définies par le service enquêteur en lien avec l'organisme. En cas de non-respect par l'organisme du plan d'action ou des échéances, l'autorité contractante ou le HFCDS peut adresser une mise en demeure à l'organisme (cf. fiche 5.6).

- d'un avis technique « d'inaptitude physique » lorsque le service enquêteur constate des carences graves dans le dispositif de sécurité. L'organisme ne peut pas détenir des informations et supports classifiés dans ses locaux.

S'il n'est pas possible de délivrer un ATAP « avec réserve », les autorités concernées (service enquêteur, autorité d'habilitation, autorité contractante) et le responsable d'organisme peuvent se réunir afin d'étudier la situation de l'organisme au regard d'une analyse de risques.

Un avis d'inaptitude interdit formellement à l'autorité contractante de transmettre des informations et supports classifiés au titulaire du contrat. Il est aussi interdit à celui-ci de produire des informations et supports classifiés.

Si le titulaire d'un contrat ne peut pas conserver dans ses locaux un avis d'aptitude classifié *Secret*, il est informé oralement des mesures recommandées par le service enquêteur qui conserve le document classifié.

Quel que soit le type d'avis émis par le service enquêteur, un avis technique d'aptitude physique est classifié au niveau *Secret*. Ce niveau de classification s'applique à l'avis comme à son annexe.

Les avis technique d'aptitude physique et attestations d'aptitude sont notifiés à la personne morale afin d'autoriser ou de refuser le début des travaux classifiés ; les références de ces documents sont communiquées à l'autorité publique contractante et à l'autorité d'habilitation.

Si les attestations ne sont pas parvenues dans le délai prédéfini ou si des carences sont constatées lors des contrôles effectués par le service enquêteur, une mise en demeure de se conformer aux prescriptions de la présente instruction est effectuée par l'autorité publique contractante. Le défaut d'exécution des travaux de mise en conformité engage la responsabilité du représentant légal de la personne morale. Cette mise en demeure est adressée en copie au service enquêteur.

Les éléments constitutifs de l'avis technique d'aptitude physique sont :

- un liminaire présentant la zone et le local ;
- une première partie présentant les éléments de l'analyse de risques réalisée par l'organisme puis les constats suivant les niveaux présentés dans la fiche

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.7

introductive du titre 5 : emprise/bâtiment, local, meuble, décision d'homologation du système de sûreté (contrôle d'accès, détection d'intrusion et vidéo-surveillance) et, le cas échéant, niveau de sûreté des systèmes classifiés ;

- une deuxième partie donnant la conclusion du service enquêteur ;
- une troisième partie (optionnelle) dédiée aux points de vigilance et aux mesures compensatoires nécessaires pour les avis « avec réserve ».

4. Modification de locaux ayant fait l'objet d'un avis technique d'aptitude physique

Toute modification (transformation des locaux, déménagement dans un autre local ou modification du dispositif de protection, etc.) implique une reconsidération de l'aptitude détenue. Le service enquêteur doit être informé de la démarche le plus tôt possible. Les éléments d'actualisation du dossier d'aptitude sont transmis au service enquêteur qui décide, si nécessaire, d'effectuer un nouveau contrôle.

Pour les personnes morales liées au ministère de la défense par contrat ou convention, la modification est signalée à l'autorité contractante par le titulaire qui fournit les éléments d'actualisation du dossier d'aptitude. L'autorité contractante saisit, le cas échéant, le service enquêteur pour diligenter, si nécessaire, un nouveau contrôle d'aptitude. En parallèle, le service enquêteur doit être informé de la démarche le plus tôt possible. Les éléments d'actualisation du dossier d'aptitude sont transmis au service enquêteur qui décide, si nécessaire, d'effectuer un nouveau contrôle

Dans l'attente du nouvel avis d'aptitude, l'autorité contractante, quelle qu'elle soit, prend les mesures nécessaires pour assurer la permanence de la protection des informations et supports classifiés.

SYNTHÈSE DES TYPES D'AVIS TECHNIQUE D'APTITUDE PHYSIQUE

Un avis technique d'aptitude physique est établi par le service enquêteur à la demande du responsable d'organisme. Il existe trois types d'avis technique d'aptitude physique présentés ci-dessous.

TYPOLOGIE	MILIEU CONCERNÉ	CONDITIONS	DUREE VALIDITE de l'ATAP	DÉTECTION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS
Avis technique d'aptitude physique « sans objection »	Milieu étatique Personne morale sous contrat ou convention avec le ministère	Niveau constaté de sûreté, avec mesures compensatoires éventuelles, répondant aux exigences de protection des informations et supports classifiés	Pas de durée de validité	Détention d'informations et supports classifiés autorisée
Avis technique d'aptitude physique « avec réserve »	Milieu étatique Personne morale sous contrat ou convention avec le ministère	Niveau constaté de sûreté ne répondant pas totalement aux exigences de protection des informations et supports classifiés et nécessitant des <u>mesures compensatoires à mettre en œuvre.</u>	De 1 à 5 ans selon le plan d'action défini	Détention d'informations et supports classifiés autorisée
Avis technique « d'inaptitude physique » (ATIP) »	Milieu étatique Personne morale sous contrat ou convention avec le ministère	Carences graves constatées dans le dispositif de sûreté	Pas de durée de validité	Détention d'informations et supports classifiés NON autorisée

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.8****ACCÈS DE PERSONNES NON QUALIFIÉES AUX LIEUX ABRITANT
DES INFORMATIONS ET SUPPORTS CLASSIFIÉS****Références :**

- Code de la commande publique – articles L.2141-6-1 et L.2141-11
- Code de la défense – articles D.3123-1 à 4, D.3126-5 à D.3126-9 et D.1221-6
- Code du travail – articles L.8112-1, L.8123-1, L.8123-4, L.8114-1 et L.8114-2
- IGI 1300 – 5.3.2 et annexe 33

Points clés

- L'accès aux lieux abritant des informations et supports classifiés à des personnes non qualifiées (personne non habilitée ou ne disposant pas du besoin d'en connaître) est possible dans les cas et conditions suivants :
 - le personnel d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence, est autorisé à procéder aux opérations requises par la situation sans être soumis aux formalités ordinaires,
 - les personnes procédant aux inspections sont autorisées par l'autorité responsable de l'emprise à pénétrer dans les zones dans lesquelles sont traités des informations et supports classifiés et font préalablement l'objet d'une vérification d'identité et d'un contrôle de leur qualité,
 - l'intervention pour une prestation de service n'est autorisée que dans le cadre d'un contrat sensible justifiant une enquête administrative préalable et comportant une clause de protection du secret.
- Si, dans ces circonstances, l'une de ces personnes accède fortuitement à une information classifiée et en prend connaissance, elle s'expose, en cas de divulgation, aux peines prévues aux articles 413-11 et 413-12 du code pénal.

L'accès de personnes **non qualifiées**¹⁸⁷ aux lieux abritant des informations et supports classifiés, qu'elles soit accompagnées ou non, n'est envisageable qu'en raison :

- de l'exécution d'une opération de secours, de sécurité ou d'incendie ;
- d'une mission de visite ou de contrôle prévue par la réglementation française, dont celle relative au travail ;
- d'inspections internationales effectuées en application d'une convention ;
- pour l'exécution d'une prestation de service ;
- dans le cadre d'une réquisition judiciaire (cf. fiche 5.9).

Ces personnes, en leur qualité particulière et pour l'exercice d'attributions conférées par la loi, ou dans un cadre contractuel, peuvent avoir à pénétrer dans les zones abritant des secrets **sans pour autant avoir la qualité ni le besoin d'accéder à ces secrets**.

¹⁸⁷ Personne qualifiée : personne disposant du besoin de connaître une information classifiée dans le cadre de sa mission et faisant l'objet d'une décision d'habilitation au niveau requis en cours de validité.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.8****1. Cas envisagés****a. Généralités**

Aucun organisme ne doit faire obstacle aux missions d'inspection, d'enquête ou de contrôle par les personnes disposant pour l'exercice de leurs attributions :

- du droit d'entrer dans les lieux où travaillent des salariés ;
- de la possibilité d'effectuer les prélèvements aux fins d'analyse ;
- de se faire présenter les livres, registres et documents utiles à l'accomplissement de leur mission.

Cependant, lorsque l'organisme détient des informations et supports classifiés, seul le responsable de l'organisme visité peut les autoriser à pénétrer dans les zones où sont traités des informations et supports classifiés, et ce après contrôle de la qualité et vérification de l'identité de ces personnes¹⁸⁸. Ces personnes ne sont nullement autorisées à accéder ou prendre connaissance d'informations et supports classifiés y compris celles appartenant à des organismes soumis à l'autorité du ministre de la défense ou à sa tutelle et des membres du corps militaire du Contrôle Général des Armées et les agents, officiers supérieurs ou fonctionnaires de catégorie A affectés au pôle travail, conformément au code de la défense (article D.3123-4 du code de la défense). Si, dans des circonstances exceptionnelles, l'un de ces intervenants accède fortuitement à des informations et supports classifiés, il est tenu de ne pas les divulguer, sous peine de s'exposer aux dispositions des articles 413-11 et 413-12 du code pénal. L'officier de sécurité de l'entité visitée rappelle préalablement à ces personnes les règles de protection du secret de la défense nationale.

b. Cas d'une mission de contrôle

Les personnes procédant aux inspections (inspecteurs et contrôleurs - y compris les membres du Contrôle Général des Armées - médecins ou inspecteurs du travail, ingénieurs de prévention, etc.) et devant pénétrer dans une zone où sont traités des informations et supports classifiés doivent être autorisées par l'autorité responsable du site, après avoir préalablement fait l'objet d'une vérification de leur identité et d'un contrôle de leur qualité¹⁸⁹. Ces personnes ne sont nullement autorisées à accéder ou prendre connaissance d'informations et supports classifiés sauf à être dûment habilitées et de justifier du besoin d'en connaître.

c. Cas de l'exécution d'une opération de secours, de sécurité ou d'incendie

Le personnel d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence avérée, est autorisé à procéder aux opérations requises par la situation sans être soumis aux formalités ordinaires.

d. Autres cas

¹⁸⁸ La présentation de leur carte professionnelle est suffisante (article R.8124-25 du code du travail).

¹⁸⁹ *Idem*.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.8

Dans tous les autres cas, l'intervention, pour une prestation de services, de personnes non qualifiées, dans un lieu abritant des éléments couverts par le secret de la défense nationale, n'est autorisée que dans le cadre d'un contrat sensible conclu par son employeur et comportant une clause de protection du secret.

Dans le cadre de l'exécution de prestation prévue par un **contrat sensible** (cf. fiche 4.3), par exemple le gardiennage de lieux abritant des éléments couverts par le secret de défense nationale, l'entretien ou la maintenance dans de telles zones, ce contrat comporte une clause de protection du secret conforme à celle figurant à l'annexe 33 de l'IGI 1300. L'autorité contractante peut compléter ou adapter la clause selon les spécificités du contrat.

Les contrats de travail des personnes exécutant un contrat sensible comportent une clause de protection du secret présentée en annexe 33 de l'IGI 1300. Lorsqu'un salarié exécutant un contrat de travail ordinaire se trouve soumis aux conditions applicables aux contrats sensibles, un avenant est introduit dans son contrat de travail.

2. Action en cas de compromission

Si une personne physique non qualifiée a eu accès à une information ou un support classifié (malveillance, espionnage, accès non justifié à des lieux abritant, etc.), il y a suspicion de compromission. La procédure à mettre en œuvre est la même que celle relevant d'une compromission avérée (cf. titre 8) et le service enquêteur est alerté au plus tôt.

**TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS****5.9****ACCÈS DES MAGISTRATS AUX INFORMATIONS ET SUPPORTS
CLASSIFIÉS****Références :**

- Code de la défense – articles L.2312-4 à L.2312-8
- Code de procédure pénale – articles 56-4, 230-2 et 698-3
- IGI 1300 – 1.2.2.2

Points clés

- Une perquisition ne peut être effectuée que par des magistrats ou des officiers de police judiciaire, selon les cas. Ils peuvent saisir des informations et supports classifiés mais ne sont pas autorisés à en prendre connaissance à ce stade de la procédure.
- Les éléments utiles à la justice sont déclassifiés avant d'être versés à la procédure. Seul le ministre de la défense peut prendre une décision de déclassification¹⁹⁰.
- Pour saisir des informations et supports classifiés dans un lieu abritant, le magistrat doit être accompagné du président de la commission du secret de la défense nationale (CSDN) ou de son représentant ou de son délégué dûment habilité.
- Seul le président de la commission du secret de la défense nationale, son représentant¹⁹¹, et, s'il y a lieu, les personnes qui l'assistent peuvent prendre connaissance d'éléments classifiés et vérifier s'ils concernent les infractions sur lesquelles portent les investigations.
- Les autorités responsables des lieux abritant des informations et supports classifiés sont tenues de diffuser à l'attention de leur personnel les consignes prescrivant la conduite à tenir en cas de perquisition, afin de faciliter le déroulement des opérations.
- Lors d'une audition, aucune personne n'est autorisée à s'exprimer au sujet d'une information classifiée avant que celle-ci ne soit déclassifiée.

Il n'est pas tenu compte dans la présente fiche de l'exception que constituent les magistrats de la formation spécialisée du Conseil d'État chargée du contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État et la défense (cf. IGI 1300 – 1.2.2.2.b).

1. Compétences

Le détenteur d'une information classifiée a le devoir d'en refuser la communication à un tiers, même s'il s'agit d'un magistrat ou d'un officier de police judiciaire. Pour être consultés par un magistrat ou un officier de police judiciaire, les éléments classifiés sont

¹⁹⁰ Pour les seuls informations et supports classifiés dont il est l'autorité émettrice.

¹⁹¹ Membre de la commission ou un délégué choisi sur une liste établie par la commission.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.9

au préalable déclassifiés sur décision du ministre¹⁹² (après avis de la commission du secret de la défense nationale).

a. Lieux abritant des éléments couverts par le secret de la défense nationale

Une perquisition envisagée dans un lieu précisément identifié comme abritant des éléments couverts par le secret de la défense nationale ne peut être effectuée que par un magistrat. Il est accompagné du président de la commission du secret de la défense nationale (ou son représentant ou délégué dûment habilité). Ils peuvent être chacun accompagnés de personnes les assistant pour procéder aux investigations. **Le responsable d'organisme accompagné de son officier de sécurité, son délégué, ou le responsable du lieu sont présents pendant la perquisition.**

Seul le président de la commission du secret de la défense nationale, son représentant ou son délégué dûment habilité et, s'il y a lieu, les personnes qui l'assistent peuvent prendre connaissance d'éléments classifiés découverts sur les lieux. Le magistrat et les personnes qui l'assistent (y compris des officiers de police judiciaire habilités pour d'autres missions) ne peuvent en aucun cas prendre connaissance d'éléments classifiés : l'administration a le devoir de s'opposer à une telle communication qui constituerait une compromission. L'accès par le magistrat ou un officier de police judiciaire à une information classifiée dématérialisée est traité comme l'accès à une information classifiée papier : seul le représentant de la commission du secret de la défense nationale est autorisé à accéder au système numérique et les modalités techniques de constitution des scellés sont adaptées.

b. Lieux « neutres »

Une perquisition dans un lieu dit « neutre », c'est-à-dire des lieux ne comportant *a priori* pas d'information et support classifié est effectuée selon les règles de droit commun, par les officiers de police judiciaire ou le magistrat. Au cours de la perquisition, l'enquêteur ne peut prendre connaissance d'éléments classifiés en cas de découverte fortuite d'informations et supports classifiés. Le magistrat, s'il n'est pas présent, en est avisé sans délai par son représentant. Le magistrat prévient alors le président de la commission du secret de la défense nationale. Les opérations sont suspendues tant que ce dernier, ou son représentant, n'est pas présent. Si ce dernier, ou son représentant, ne peut se déplacer pour assister physiquement à la perquisition, le magistrat ou l'officier de police judiciaire transmet à la commission du secret de la défense nationale les documents placés sous scellés par tout moyen en conformité avec la réglementation applicable au secret de la défense nationale.

Le déroulement d'une procédure de perquisition est précisé à l'article 56-4 du code de procédure pénale et dans l'IGI 1300.

¹⁹² À l'exception des informations et supports classifiés dont il n'est pas l'autorité émettrice, celles-ci devant faire l'objet préalablement à toute consultation d'une déclassification par l'autorité compétente.

TITRE 5 : SÉCURITÉ DES LIEUX ABRITANT DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

5.9

2. Conduite à tenir en cas de perquisition

L'autorité responsable du site – ou son officier de sécurité – définit une procédure et transmet aux personnes affectées sur le site des consignes relatives à la conduite à tenir en cas de perquisition, tout particulièrement lorsqu'il s'agit d'un lieu référencé comme « abritant » des informations et supports classifiés. Elles visent à faciliter le bon déroulement de l'opération tout en garantissant la protection du secret :

- a. demander au magistrat la **décision de perquisition** qui doit être écrite et motivée : elle doit indiquer la nature des infractions sur lesquelles portent les investigations, les raisons et l'objet de la perquisition et les lieux précisément visés par la perquisition. En parallèle, **informer dans les meilleurs délais sa hiérarchie** de la procédure judiciaire ;
- b. **relever l'identité** des personnes et s'assurer que les lieux perquisitionnés sont bien ceux inscrits sur la décision de perquisition (des confusions sont possibles) ;
- c. s'il s'agit d'un lieu abritant, s'assurer de la présence du magistrat et du président de la commission du secret de la défense nationale (ou de son représentant ou délégué dûment habilité). Les opérations de perquisition ne peuvent débuter qu'en leur présence ;

cas 1 : Si les nécessités de l'enquête justifient que les éléments classifiés soient saisis en original, des copies sont laissées à leur détenteur. Les éléments éventuellement saisis sont remis au président de la commission du secret de la défense nationale ou son représentant ou délégué dûment habilité et placés sous scellés durant les opérations, sans que le magistrat ou l'officier de police judiciaire ait pu prendre connaissance de leur contenu. En effet, ils ne peuvent être versés à la procédure qu'après déclassification. La réalisation des copies et la saisie des documents classifiés originaux doivent faire l'objet d'un marquage, d'un enregistrement et d'un suivi par bordereau ;

cas 2 : si des informations et supports classifiés sont découverts dans un lieu neutre, l'officier de police judiciaire avise immédiatement le magistrat mandant. Le président de la commission du secret de la défense nationale est alerté et les documents saisis lui sont transmis. L'officier de sécurité s'assurera que des copies soient conservées par le détenteur. Les informations et supports classifiés sont placés sous scellés durant les opérations, sans que le magistrat ou l'officier de police judiciaire ait pu prendre connaissance de leur contenu. En effet, ils ne peuvent être versés à la procédure qu'après déclassification ;

- d. **rendre compte à sa hiérarchie** du déroulement de la perquisition.

3. Cas particulier des auditions

Aucune autorité administrative ne peut autoriser l'un de ses agents à s'exprimer au sujet d'une information classifiée avant que celle-ci ait été préalablement déclassifiée. Si une autorité judiciaire interroge une personne sur des éléments couverts par le secret de la défense nationale, celle-ci doit donc refuser de répondre en rappelant les dispositions applicables en matière de protection du secret de la défense nationale.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ

INTRODUCTION : REMARQUES GÉNÉRALES

Le présent titre 6 ne s'applique qu'aux organismes contractants avec le ministère de la défense et la direction des applications militaires du CEA (CEA/DAM) pour les systèmes d'information qu'ils exploitent dans l'exécution du contrat, quel qu'en soit le niveau de classification, dénommées ci-après personnes morales ou entités. Ce titre s'inscrit en complément des réglementations en vigueur (IGI 1300, II 901, dispositif SAIV, etc.) sans se substituer à ces dernières. Il précise ces différentes réglementations, vise à harmoniser et à détailler les interactions entre les parties à un contrat aux termes duquel des informations ou supports sensibles sont impliqués. Dans certains cas, il rappelle des mesures particulières de la réglementation et peut apporter des mesures complémentaires.

En ce qui concerne les systèmes livrés par les personnes morales contractantes, les dispositions contractuelles s'appliquent. Sauf disposition contraires, le système livré doit être conforme à la réglementation pour le niveau de classification des informations qu'il traitera en exploitation par le ministère.

Pour les plateformes représentatives ou de qualification des systèmes d'armes détenues par les industriels devant rester similaires aux systèmes opérationnels qu'elles représentent, les exigences de sécurité numérique qui leur sont applicables sont définies par contrat. Les industriels sont tenus d'en assurer la sécurité physique.

Les organismes relevant du ministère de la défense doivent appliquer l'IM 7326 (politique de sécurité des systèmes d'information). Les établissements publics sous tutelle du ministère de la défense appliquent également l'IM 7326, sous réserve des précisions arrêtées par le ministre à leur endroit.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.1****CARTOGRAPHIE DES SYSTÈMES D'INFORMATION DES PERSONNES MORALES DE DROIT PRIVÉ CONTRACTANTES****Références :**

- Code de la défense – articles L.1332-6-1 à L.1332-6-6
- IGI 1300 – 6.1
- II n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- Cartographie du système d'information – guide de l'ANSSI d'élaboration en 5 étapes

Points clés

- La cartographie permet une connaissance complète des systèmes d'information de l'organisme contractant (cf. annexe 22).
- Le contenu de la cartographie est précisé dans la politique de sécurité numérique de l'organisme contractant.

La cartographie apporte une connaissance complète de l'environnement du système numérique (SN), de ses interactions avec l'extérieur et de toute son infrastructure technique. Cette connaissance détaillée permet de réagir plus efficacement en cas d'incident (cf. fiche 8.2).

La cartographie des systèmes numériques est établie sous la responsabilité de l'autorité qualifiée pour la sécurité des systèmes d'information. Elle fournit la connaissance du système numérique global de l'entité (**classifié et non classifié**) et permet notamment d'appréhender les principaux risques sur son activité. Cette cartographie est également nécessaire à l'identification initiale des Systèmes d'Information d'Importance Vitale (SIIV) et des systèmes d'information traitant des informations sensibles, *Diffusion Restreinte* ou classifiées et de manière plus générale, à la catégorisation des systèmes numériques.

L'autorité qualifiée en SSI de l'organisme contractant précise dans la politique de sécurité numérique le contenu exact de la cartographie qui doit être rendu disponible :

- la description fonctionnelle et les lieux d'installation de chaque système numérique et de ses différents sous-réseaux et, le cas échéant, les plages d'adresses associées aux différents sous-réseaux composant le système numérique ;
- la description fonctionnelle des points d'interconnexion du système numérique et de ses différents sous-réseaux avec des réseaux tiers, notamment la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions ;
- l'inventaire et l'architecture des dispositifs d'administration du système numérique permettant de réaliser notamment les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ;
- la typologie des équipements actifs de réseau ;

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.1**

- la typologie des comptes disposant de droits d'accès privilégiés au système numérique. Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés ;
- les équipements d'import et d'export de données ;
- l'inventaire, l'architecture et le positionnement des services de communication et d'accès distant mis en œuvre par le système numérique.

Les éléments de cartographie ainsi réunis sont des documents sensibles susceptibles de contenir des informations couvertes par le secret de la défense nationale.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2****LE PROCESSUS D'HOMOLOGATION****Références :**

- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 dite « NIS » (Network and Information Security)
- Code de la défense – articles L.1332-6-1 à L.1332-6-6 et L.1332-41-1 à 2
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, dite « loi informatique et libertés » (LIL), mise à jour par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, complétée par ses décrets d'application
- IGI 1300 – 6.1
- II n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- Référentiel général de sécurité – version 2.0 du 13 juin 2014

Points clés

- L'homologation d'un système numérique consiste à évaluer les risques encourus afin de les traiter ou d'accepter ceux ayant un caractère résiduel. Elle fournit un niveau de confiance dans l'usage et la protection des informations et du système numérique.
- La démarche d'homologation est un préalable à toute mise en service d'un système numérique, quel que soit son niveau de sensibilité ou de classification.
- La démarche d'homologation est globale : elle doit prendre en compte l'écosystème métiers et technologies de l'information, aussi bien interne qu'externe, dans lequel le système numérique concerné s'intègre dans toutes ses phases de vie.
- La démarche d'homologation doit être adaptée aux enjeux et à la nature du système numérique.

1. La démarche d'homologation

La démarche d'homologation s'intègre dans le cycle de vie d'un système numérique. Elle repose sur une analyse de risques globale et prend en compte tous les éléments indispensables au fonctionnement et à la sécurité du système. Elle permet de s'assurer que les risques pesant sur ce système, dans son contexte d'emploi, sont connus et maîtrisés. À cet effet, elle consiste à trouver le juste équilibre entre les risques résiduels acceptables, les actions à conduire pour la sécurisation et les contraintes techniques ou organisationnelles, en prononçant les arbitrages nécessaires, de manière formelle, par un responsable qui a autorité pour le faire.

L'homologation de sécurité d'un système numérique correspond à une démarche globale : le périmètre du système numérique à homologuer comporte tous les éléments

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2**

indispensables au fonctionnement et à la sécurité du système. Il inclut les éléments fonctionnels et d'organisation, les éléments techniques, ainsi que le périmètre géographique et physique. L'homologation tient compte de l'environnement numérique du système comme les systèmes en interface, les équipements externes pouvant être connectés au système, notamment lors d'opération de maintenance, etc.

La démarche d'homologation débute par la définition de la stratégie d'homologation qui a pour objectif de préciser :

- la cible de l'homologation (le périmètre du système, le ou les référentiels réglementaires applicables) ;
- les étapes de la démarche d'homologation ;
- les acteurs concernés, les actions à réaliser et les livrables attendus ;
- la liste des documents constituant le dossier d'homologation.

La stratégie d'homologation peut être commune à plusieurs systèmes d'information, permettant ainsi de mettre en place une démarche d'homologation et de gestion des risques cohérente sur un système plus global (par exemple, sur des systèmes numériques partageant un même contexte : même lieu, même métier, même projet, etc.) ou lorsque cela est de nature à simplifier les travaux à réaliser (par exemple lorsque les systèmes d'information partagent un même socle de sécurité). Les décisions d'homologation doivent cependant être enregistrées séparément pour chaque système.

La stratégie d'homologation doit faire l'objet d'une validation formelle par l'autorité d'homologation. Pour les systèmes d'information classifiés et pour les systèmes *Diffusion Restreinte* les plus exposés et critiques (cf. catégorisation des systèmes numériques mentionnée ci-dessus), la validation de la stratégie d'homologation est faite en accord avec l'autorité contractante sur avis du service enquêteur. La validation de la stratégie d'homologation doit intervenir au plus tôt du cycle de vie du système, idéalement dès la phase de conception.

La démarche d'homologation doit être adaptée aux enjeux et éviter la « sur-sécurité » ou encore la multiplication de documents fastidieux, inadaptés ou inefficaces.

Il convient donc de catégoriser les systèmes numériques pour éviter de conduire des démarches d'homologation complexes, coûteuses et finalement inadaptées à leurs besoins de sécurité. La catégorisation du système numérique dépend essentiellement de deux paramètres : son exposition et sa criticité.

Les méthodes et critères précis de catégorisation sont définis par l'autorité qualifiée d'un système. La catégorisation d'un système numérique est validée formellement par l'autorité qualifiée, en accord avec l'autorité contractante.

Un exemple de catégorisation est proposé en annexe (cf. [annexe 22](#)).

Afin de simplifier le processus, la personne morale de droit privé peut définir des stratégies types d'homologation adaptées à la catégorisation des systèmes numériques choisie.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2**

En accord avec l'autorité contractante et le service enquêteur, des démarches adaptées peuvent être envisagées par catégorie de système numérique : des simplifications systémiques de démarche ou de dossier, voire des dérogations, peuvent être envisagées pour les systèmes numériques les moins exposés et les moins critiques.

La démarche d'homologation pourra distinguer une homologation de référence du système numérique et une ou des homologations de déploiement.

L'homologation de référence est une homologation type qui ne prend pas en compte les spécificités des développements locaux.

L'homologation de déploiement est la décision préalable à l'exploitation du système numérique attestant de la conformité à l'homologation de référence et, le cas échéant, du traitement des non-conformités. Elle précise les conditions de déploiement.

La rédaction de la stratégie d'homologation peut s'appuyer sur le guide de l'ANSSI portant sur l'homologation¹⁹³.

La démarche d'homologation s'appuie sur une analyse de risques qui décrit et caractérise particulièrement :

- la menace « cyber » contextualisée pesant sur le système numérique, notamment les sources de risque intentionnel (profils d'attaquant, objectifs visés, etc.) ;
- le niveau de dangerosité des parties prenantes de l'écosystème du fait des interactions métiers et IT qu'elles entretiennent avec le système numérique dans ses différentes phases de vie ;
- les scénarios de risques intentionnels décrivant les chemins d'attaque et les modes opératoires susceptibles d'être orchestrés par les sources de risque, y compris *via* les parties prenantes de l'écosystème (attaques par rebond, *supply chain attacks*, etc.).

Il est recommandé de réaliser l'analyse de risque selon la méthode EBIOS Risk Manager de l'ANSSI, pour les systèmes les plus exposés et critiques. Une méthode simplifiée peut être utilisée pour les systèmes les moins exposés et les moins critiques.

2. L'autorité d'homologation

Pour les systèmes d'information appartenant ou mis en œuvre par un opérateur privé, l'autorité d'homologation est désignée dans les conditions suivantes :

- dans le cas où le système numérique traite d'informations classifiées au niveau *Très Secret* « classification spéciale », le SGDSN est l'autorité d'homologation ;
- dans le cas où le système numérique est amené à traiter des informations et supports classifiés de l'UE, y compris au niveau *Restricted-UE/EU-Restricted*, ou de l'OTAN, l'autorité d'homologation est le SGDSN ou toute autre autorité à laquelle il délègue cette responsabilité ;
- pour les systèmes d'information classifiés utilisés par des organismes relevant de son périmètre au titre de l'article 2 du décret n° 2012-383 du 20 mars 2012, l'autorité d'homologation est le SGDSN ;
- dans le cas d'une interconnexion entre un système numérique *Secret* ou *Très Secret* et un système numérique d'un niveau de classification différent ou non classifié, si

¹⁹³ Disponible sur le site : cyber.gouv.fr.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ

6.2

l'utilisation de dispositifs agréés est impossible, l'autorité d'homologation est le SGDSN ou toute autorité qu'il désigne ;

- dans le cas d'une passerelle entre un système numérique *Secret* ou *Très Secret* et un système numérique qui n'est pas sous maîtrise nationale, si l'utilisation de dispositifs agréés est impossible, l'autorité d'homologation est l'ANSSI ou toute autorité qu'elle désigne ;
- dans les autres cas, notamment lorsque le système numérique traite d'informations non classifiées ou classifiées au niveau *Secret* ou *Très Secret*, la désignation de l'autorité d'homologation relève de la responsabilité de l'autorité qualifiée en sécurité des systèmes d'informations de la personne morale.

L'autorité d'homologation prend la décision d'accepter les risques résiduels ; lorsque cela est possible, elle doit être l'autorité chargée de l'emploi du système ou située dans la chaîne d'emploi du système.

Il est possible de distinguer l'autorité d'homologation qui prononcera l'homologation de référence d'un système et l'autorité (ou les autorités) d'homologation qui prononcera les homologations de déploiement.

3. Réglementation applicable

Certaines procédures et mesures de sécurité sont imposées, *a priori*, sur le système par la loi ou les règlements afin d'instaurer un socle jugé minimal de sécurité pour les systèmes numériques soumis à la présente instruction.

En fonction de la nature du système numérique objet de l'homologation, il peut être parfois impossible pour des raisons techniques ou opérationnelles de se conformer à certaines mesures de sécurité. Par exemple, l'authentification forte de l'utilisateur sur un système d'arme comme un missile air-air peut apparaître peu pertinente. Les non conformités éventuelles doivent figurer dans le dossier d'homologation, doivent y être justifiées et les éventuels risques associés doivent être identifiés.

Lorsque plusieurs réglementations s'appliquent sur un même SI, la démarche d'homologation et la décision d'homologation sont uniques et couvrent l'ensemble des réglementations applicables.

4. Le dossier d'homologation

La composition du dossier d'homologation est fixée dans la stratégie d'homologation. Il est composé *a minima* :

- d'une description du système numérique (son utilité, son cadre d'emploi, les composants matériels et logiciels, l'architecture réseau logique et physique, les acteurs, administrateurs et responsables de sécurité, les références des plans contractuels) ;
- de l'évaluation des risques résiduels ;
- du plan d'amélioration continu de la sécurité.

Pour les systèmes d'information classifiés, le dossier d'homologation comprend en outre :

- les avis techniques d'aptitude physique (ATAP) ;

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2**

- sauf dérogation du service enquêteur et de l'autorité contractante, l'avis technique d'aptitude informatique (ATAI) (cf. fiche 6.3).

Selon le cadre réglementaire applicable et la catégorie des systèmes d'information, le dossier d'homologation est également composé de :

- l'analyse de risques et les mesures de mitigation envisagées ;
- les objectifs de sécurité du système numérique ;
- la politique de sécurité du système numérique¹⁹⁴ ;
- les procédures d'exploitation de la sécurité (PES) ;
- les modalités de gestion des risques résiduels ;
- les résultats des tests et des audits menés pour vérifier l'état de sécurité du système ;
- la documentation de sécurité à destination des utilisateurs et des administrateurs ;
- la documentation relative à la gestion des éléments cryptographiques mis en œuvre dans le système numérique ;
- la cartographie complète du système numérique qui comprend notamment la liste des équipements externes pouvant être connectés au système numérique (matériel de maintenance, d'audit, etc.) ;
- les schémas détaillés de l'architecture du système numérique ;
- la référence des agréments des dispositifs de sécurité.

La nécessité de joindre chacun de ces documents au dossier d'homologation est évaluée et justifiée au regard des enjeux du système numérique. Si un document n'est pas versé au dossier d'homologation, la justification associée y figure.

Le dossier d'homologation, particulièrement la politique de sécurité du système numérique et le plan d'amélioration continue de la sécurité, présente les mesures de sécurité en profondeur suivantes :

- protection : mesures visant à réduire les vulnérabilités et facteurs d'exposition du système numérique (surface d'attaque) ;
- défense : mesures visant à superviser le système numérique, détecter les événements de sécurité et anticiper la réponse à un incident ;
- résilience : mesures visant à gérer les situations de crise et à assurer la continuité et reprise d'activité ;
- gouvernance : mesures visant à définir une organisation de management des risques « cyber » adaptée, agile et réactive pour le système numérique.

5. Commission d'homologation

L'autorité d'homologation met en place une commission d'homologation chargée de l'assister et de préparer la décision d'homologation. Cette commission comprend notamment des représentants des utilisateurs du système et des responsables de l'exploitation et de la sécurité du système.

¹⁹⁴ Généralement, il s'agit d'une politique de sécurité des systèmes numériques applicable au sein de l'organisme éventuellement complété d'éléments propres au système numérique considéré.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2**

Pour les SI classifiés, le service enquêteur et le fonctionnaire de sécurité des systèmes d'information (FSSI) du ministère de la défense sont membres de droit de la commission. Pour les autres SI, ils sont systématiquement informés et membres de la commission si nécessaire. Les contractants ainsi que l'autorité contractante de premier rang sont membres de droit des commissions d'homologation. Afin de leur permettre d'apprécier la nécessité de leur participation, l'autorité d'homologation les informe, dans un délai raisonnable, de la date de la commission et leur transmet le dossier d'homologation sauf avis contraire.

Au titre de la maîtrise du risque « cyber » au sein des entreprises de défense, la DGA doit pouvoir accéder, si nécessaire, aux informations concernant l'état de cybersécurité des systèmes numériques soumis à la présente instruction et participer aux commissions d'homologation de ces systèmes numériques.

En tant qu'autorité nationale en matière de sécurité des systèmes d'information, l'ANSSI conserve la possibilité, sur son périmètre de responsabilité, de participer à toute commission d'homologation d'un système numérique classifié. Elle en est membre de droit lorsque le SGDSN est l'autorité d'homologation.

Le fonctionnaire de sécurité des systèmes d'information peut participer à toutes les commissions d'homologation des systèmes numériques soumis à la présente instruction.

6. Décision d'homologation

La décision d'homologation constitue le premier aboutissement de la démarche d'homologation, le cas échéant après avis de la commission d'homologation. Elle se traduit par l'attestation formelle de l'autorité d'homologation que le système numérique considéré est protégé conformément aux objectifs de sécurité fixés et précise les éventuelles conditions d'emploi. Ces objectifs sont généralement exprimés en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité.

L'autorité d'homologation accepte les risques résiduels de sécurité, en pleine connaissance des vulnérabilités du système numérique qui sont liées notamment :

- aux usagers ;
- aux interconnexions avec d'autres systèmes ;
- aux supports amovibles ;
- aux accès à distance par des utilisateurs en mobilité ;
- aux moyens de visualisation et d'hébergement des informations et supports classifiés ;
- aux opérations de maintenance, d'exploitation ou de télégestion du système, notamment lorsqu'elles sont effectuées par des prestataires externes.

Un système numérique classifié protège des informations, soit transmises par le ministère de la défense pour l'exécution du contrat, soit élaborées dans le cadre du contrat au profit du ministère. La compromission de ces informations est de nature à remettre en cause les intérêts fondamentaux de la Nation. Par ailleurs, la perte d'intégrité d'une information sur des systèmes numériques protégeant des informations de niveau *Diffusion Restreinte* ou classifié peut entraîner le sabotage d'un système d'armes (rendre le système d'armes non fonctionnel, non conforme aux performances attendues, non intègre, permettre sa prise de contrôle par un attaquant).

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2**

L'autorité d'homologation n'est pas autorisée à prononcer l'homologation d'un système numérique soumis à la présente instruction, si le service enquêteur et l'autorité contractante constatent un défaut de sécurité, de nature à remettre en cause l'exécution de ses missions par le ministère de la défense. Ce défaut peut se caractériser par la mise en péril de la confidentialité, la disponibilité ou l'intégrité des informations, y compris non protégées.

La décision d'homologation doit intervenir avant la mise en service opérationnelle du système.

La décision d'homologation est prononcée pour une durée maximale :

- de cinq ans pour un système numérique traitant d'informations non protégées, sensibles ou *Diffusion Restreinte* ;
- de trois ans pour un système numérique de niveau *Secret* ;
- de deux ans pour un système numérique de niveau *Très Secret* ou traitant d'informations classifiées de niveau *Très Secret* classification spéciale.

Cette durée d'homologation peut être réduite par une réglementation plus contraignante, comme celle concernant les systèmes d'information d'importance vitale ou par décision d'une autorité d'homologation.

Le service enquêteur et l'autorité contractante sont destinataires de toute décision d'homologation¹⁹⁵. Elles peuvent demander le dossier d'homologation correspondant.

7. Contrôle et renouvellement de l'homologation

Conformément aux instructions de la PSSI de la personne morale, l'autorité d'homologation fixe les conditions du maintien de l'homologation de sécurité au cours du cycle de vie du système numérique. Elle contrôle régulièrement que le système fonctionne effectivement selon les conditions qu'elle a approuvées, en particulier après des opérations de maintien en condition opérationnelle et de maintien en condition de sécurité (MCS).

L'autorité d'homologation examine le besoin de renouvellement de l'homologation avant le terme prévu sur la base du dossier tenu à jour par le responsable de la Sécurité du système numérique lorsque :

- les conditions d'exploitation du système ont été significativement modifiées ;
- des nouvelles fonctionnalités ou applications ont été installées ;
- le système a été interconnecté à de nouveaux systèmes ;
- des problèmes d'application des mesures de sécurité ou des conditions de maintien de l'homologation ont été révélés ;
- les menaces sur le système ont évolué ;
- de nouvelles vulnérabilités ont été découvertes ;
- le système a fait l'objet d'un incident de sécurité ;

¹⁹⁵ Les décisions d'homologation relatives aux entités contractantes avec la DGSE répondent à une procédure spécifique.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.2**

- un avis technique d'aptitude informatique défavorable est émis ou, à la demande conjointe du service enquêteur et de l'autorité contractante, si un avis technique d'aptitude informatique présente des réserves.

Le responsable de la sécurité du système numérique analyse les événements pouvant remettre en cause l'homologation et, si les évolutions génèrent des risques supplémentaires pour la sécurité du système numérique, il sollicite l'autorité d'homologation *via* la commission d'homologation pour la conduite à tenir. L'analyse est versée au dossier d'homologation.

L'autorité d'homologation est responsable du contrôle du niveau de sécurité atteint du système à travers l'audit qu'elle réalise ou fait réaliser (cf. fiche 6.4).

Le service enquêteur, l'autorité contractante ou l'autorité d'habilitation peuvent contrôler eux-mêmes ou faire contrôler le niveau de sécurité atteint et la maîtrise des risques du système. Dans le cas d'un système classifié, si ce contrôle est réalisé par la DRSD, il donne lieu à un ou plusieurs avis technique d'aptitude informatique. Dans un système de niveau *Diffusion Restreinte*, le contrôle donne lieu à un avis sur le niveau de sécurité et, si besoin, à des recommandations.

Sauf dérogation de la DRSD et de l'autorité contractante, le renouvellement d'une homologation nécessite un nouvel avis technique d'aptitude informatique.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.3****CONTRÔLE D'APTITUDE AU TRAITEMENT D'INFORMATIONS NUMÉRIQUES CLASSIFIÉES****Références :**

- IGI 1300 – annexe 30
Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 sur la protection contre les signaux parasites compromettants

Points clés

- Les systèmes d'information classifiés sont homologués avant d'être utilisés. Dans ce cadre, un avis technique d'aptitude informatique (ATAI) est nécessaire sauf dérogation prévue par la présente fiche.
- L'avis technique d'aptitude informatique est émis par le service enquêteur et informe les autorités contractantes et l'autorité d'homologation du niveau de protection atteint sur le système numérique de l'entité.

1. Généralités

Pour les SI classifiés intéressant la défense, le service enquêteur contrôle le niveau de sécurité et s'assure que les risques « cyber » sont maîtrisés. Ce contrôle donne lieu à un ou plusieurs avis. Un avis technique d'aptitude informatique est généralement nécessaire dans le cadre de l'homologation ou des renouvellements d'homologation.

Afin de produire un avis technique d'aptitude informatique, le service enquêteur s'assure que les mesures suivantes ont été prises :

- pour les contrats classifiés intéressant la défense, le niveau de classification du système numérique est conforme aux prescriptions du plan contractuel de sécurité attaché au contrat ;
- les constituants physiques du système numérique sont situés dans des locaux ayant fait l'objet d'un avis technique d'aptitude physique et que, le cas échéant, le câblage informatique cheminant hors de ces locaux respecte les règles décrites dans la fiche 6.10 ;
- un contrôle de conformité a été réalisé pour les mesures de protection contre les signaux parasites compromettants ;
- les personnes ayant accès au système numérique ou à ses constituants physiques sont habilitées au niveau idoine ;
- les supports numériques classifiés sont dûment enregistrés.

Pour les systèmes d'information de niveau *Très Secret*, le service enquêteur s'assure de plus que :

- les résultats de mesures d'atténuation électromagnétiques (Tempest) réalisées par un organisme accrédité identifient les locaux utilisés comme aptes à traiter des informations numériques classifiées au niveau *Très Secret* en fonction des caractéristiques des équipements présents ;
- les locaux identifiés sont érigés en zone réservée incluse dans une zone protégée.

L'élaboration de l'avis technique d'aptitude informatique est réalisée sur la base d'une évaluation *in situ* préparée à partir de documents prévus dans le dossier

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.3**

d'homologation (notamment le document de description du système numérique et des informations du DSSI).

2. Le dossier de sécurité d'un système d'information (DSSI)

Le dossier de sécurité d'un système d'information est un dossier d'identité et de description d'un système numérique.

Le dossier de sécurité d'un système d'information est l'une des pièces constitutives du dossier d'homologation. Il est constitué des informations visant à décrire les éléments mentionnés à l'annexe 23 de la présente instruction ainsi que dans le PCS.

Une version complète et à jour du dossier de sécurité d'un système d'information doit pouvoir être fournie dans des délais brefs à la demande de l'autorité contractante, de l'autorité d'habilitation ou du service enquêteur. Il contient les informations nécessaires pour connaître un système dans le cadre d'une inspection, d'un contrôle, d'un audit, d'un avis technique d'aptitude informatique, d'une intervention de l'État dans le cadre d'un incident.

Pour faciliter la constitution du dossier de sécurité d'un système d'information, certains documents (ou extraits de documents) existants par ailleurs et permettant de fournir les informations requises peuvent être référencés et joints.

Le niveau de sensibilité du dossier de sécurité d'un système d'information est précisé dans le PCS attaché au contrat.

3. Évaluation de l'aptitude technique informatique

Le service enquêteur réalise *in situ* et en tant que de besoin des contrôles sur les conformités réglementaires. Il apprécie l'efficacité et la complétude des mesures de sécurité déployées par l'entité visant à réduire les risques identifiés et à se conformer à la réglementation applicable et aux bonnes pratiques. Le service enquêteur notifie l'avis qu'il a élaboré à la personne morale et à l'autorité contractante.

a. Avis favorable

Le niveau de sécurité est jugé satisfaisant et les risques « cyber » semblent maîtrisés.

b. Avis avec réserves

Le niveau de sécurité n'est pas jugé satisfaisant ou la maîtrise des risques « cyber » doit être améliorée.

Des réserves peuvent être formulées en cas :

- d'absence de fourniture par la personne morale d'un ou plusieurs documents nécessaires à l'évaluation du système numérique par le service enquêteur dans des délais compatibles avec l'exécution du contrat classifié ;
- de non-conformité réglementaire ;

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.3**

- d'identification de lacunes techniques ou organisationnelles faisant peser sur les informations et supports classifiés de défense un risque non négligeable.

Un plan d'action est élaboré par la personne morale afin de traiter les points faisant l'objet des réserves, dont l'avancement est présenté en commission d'homologation.

c. Avis défavorable

La mise en lumière de vulnérabilités graves ou de non conformités réglementaires mettant en péril la confidentialité, la disponibilité, l'intégrité ou la traçabilité d'informations et supports classifiés de défense peuvent conduire le service enquêteur à émettre un avis défavorable.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.4****LES AUDITS DE SÉCURITÉ****Références :**

- Code de la défense – articles L.1332-6-1 à L.1332-6-6
- IGI 1300 – 6.6.3.1 et 6.9
- II n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Les audits de sécurité interviennent aux moments critiques du cycle de vie d'un système numérique :
 - lors de l'homologation initiale ou à l'occasion du renouvellement de cette dernière,
 - à des fins de maintien en condition de sécurité du système numérique.
- Les audits peuvent être externalisés, notamment auprès de prestataires qualifiés par l'ANSSI – les prestataires d'audit SSI (PASSI).
- L'externalisation des audits de systèmes d'information classifiés est possible après analyse de risques et avec l'accord de l'autorité contractante.

En complément des tâches de maintien en condition de sécurité, l'autorité d'homologation réalise ou fait réaliser périodiquement des contrôles ou des audits¹⁹⁶ de sécurité des systèmes d'information. Pour les systèmes sensibles et classifiés un audit de sécurité est obligatoire avant l'homologation et chaque renouvellement d'homologation.

Une autorité qualifiée pour la sécurité des systèmes d'information de la personne morale peut s'appuyer sur des prestataires de services internes ou externes pour la réalisation d'audits SSI. En ce qui concerne les systèmes classifiés de défense, l'externalisation est possible après analyse de risques et avec l'accord de l'autorité contractante.

Sauf dérogation de l'autorité contractante, les auditeurs d'un système numérique *Diffusion Restreinte* doivent être habilités au niveau *Secret*. Les auditeurs d'un système numérique classifié doivent être habilités au niveau *Très Secret*. Lorsqu'il s'agit d'un auditeur interne, ce niveau d'habilitation est sans incidence sur le niveau d'habilitation

¹⁹⁶ Processus systématique, indépendant et documenté en vue d'obtenir des enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères de contrôle ou d'audit et sont vérifiables et de les évaluer de manière objective pour déterminer dans quelle mesure les critères de sécurité sont satisfaits. Un audit de sécurité peut comporter un audit d'architecture, un audit de configuration, un audit de code source, un audit organisationnel et un test d'intrusion. Un contrôle de sécurité comporte un audit de configuration et un audit de conformité à la documentation applicable au système numérique.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.4**

de la personne morale. En cas de sous-traitance de la prestation d'audit, le contrat doit comporter un plan contractuel de sécurité validé par l'autorité contractante.

Ces audits de sécurité doivent, en plus de la conformité aux règles en vigueur, évaluer le niveau de robustesse des systèmes visés face à l'état de l'art des menaces informatiques.

Les auditeurs réalisant l'audit de sécurité utilisent les outils logiciels, outils matériels et privilèges qu'ils estiment nécessaires à la réalisation des activités d'analyse technique conformes à l'état de l'art.

Les conditions d'utilisation des équipements nécessaires à l'audit doivent respecter la fiche 6.7 relative à la mobilité et aux supports amovibles.

Pour un système *Diffusion Restreinte* ou classifié, en cas de recours à un prestataire, celui-ci doit être qualifié « Prestataire d'Audit de la Sécurité des Systèmes d'Information » (selon la nature du système numérique: PASSI ou PASSI-LPM¹⁹⁷). Le plan contractuel de sécurité du sous-contrat doit préciser comment la prestation d'audit doit être réalisée (il peut prévoir l'impossibilité pour les auditeurs de récupérer des informations issues du système numérique audité, la mise à disposition par la personne morale auditée des moyens d'audit ou des moyens pour rédiger le rapport d'audit, la réalisation complète de la prestation dans les locaux de la personne morale auditée, l'exécution des outils d'audit par les administrateurs du système et non par les auditeurs, la réalisation de la totalité de la prestation par des moyens logiciels ou matériels propres aux auditeurs mais avec des mesures de contrôle et de surveillance particulières, etc.).

Les rapports d'audit sont classifiés¹⁹⁸.

L'audit porte au moins sur :

- l'application des dispositions réglementaires et des directives particulières de l'autorité qualifiée en sécurité des systèmes d'information responsable ;
- le respect des conditions organisationnelles et techniques prévues par l'homologation du système ;
- l'adéquation des règles d'exploitation (contrôle des procédures d'exploitation de sécurité) ;
- la protection du personnel ;
- les mesures de sauvegarde en cas d'incident ou d'accident ;
- la planification des mesures particulières relatives aux situations de crise ;
- l'évaluation des conséquences des risques acceptés ;
- le respect des dispositions réglementaires relatives à la gestion des articles contrôlés de la sécurité des systèmes d'information ;
- la protection contre les signaux parasites compromettants.

Les conditions de mise à disposition des outils, des privilèges et de communication des relevés techniques nécessaires à la réalisation de l'audit de sécurité doivent figurer dans une charte d'audit spécifique au système visé, quel que soit son niveau de classification

¹⁹⁷ Prestataire d'audit qualifié par l'ANSSI au sens des articles L.1332-6-1 à L.1332-6-6 du code de la défense.

¹⁹⁸ Si la personne morale n'est pas habilitée, le rapport d'audit n'est pas classifié mais doit porter la mention *Diffusion Restreinte*. Dans ce cas, les noms des systèmes numériques ne sont pas cités et les vulnérabilités non détaillées.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.4**

et sans préjudice des dispositions de la présente instruction. Cette charte d'audit entre l'organisme responsable du système numérique visé et celui réalisant l'audit précise ces conditions et le périmètre de l'audit.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.5****SOUS-CONTRACTANCE À UN TIERS EN MATIÈRE INFORMATIQUE****Références :**

- Code de la commande publique
- IGI 1300 – 6.3
- Guide de l'externalisation par l'ANSSI

Points clés

- Pour les systèmes d'information classifiés ou *Diffusion Restreinte*, le recours par un contractant du ministère de la défense à une sous-contractance informatique doit être explicitement autorisé par le plan contractuel de sécurité initial.
- Préalablement à la mise en place d'une sous-contractance, une analyse de risques doit être menée.
- La contractualisation par le cocontractant à un tiers d'activités sur des systèmes d'information sensibles, *Diffusion Restreinte* ou classifiés impose de formaliser les objectifs de sécurité dans des documents dédiés et d'appliquer les mesures de protection associées.

La sous-contractance informatique consiste à confier à un tiers tout ou partie de l'activité dans le domaine des systèmes d'information. Ainsi, le cocontractant peut également avoir recours à des services reposant sur des infrastructures mutualisées. Il peut s'agir, entre autres, de MCO (maintien en condition opérationnelle), de MCS (maintien en condition de sécurité), de TMA (tierce maintenance applicative), d'ASP (*Application Service Provider* - fournisseur d'applications en ligne), de SAAS (*Software as a service* - logiciel en tant que service), de MSSP (*Managed Security Service Provider* - fournisseur de service de sécurité géré), capacité de calcul, hébergement de données, etc. Toute personne morale sous contrat avec le ministère de la défense traitant des informations *Diffusion Restreinte* ou classifiées est tenue d'appliquer les présentes dispositions. **Le recours à une sous-contractance doit être explicitement autorisé dans le plan contractuel de sécurité.**

Le cas échéant, certaines activités peuvent être identifiées comme des tâches essentielles ne pouvant faire l'objet d'une sous-contractance¹⁹⁹. En particulier, les prestations d'administration de la sécurité d'un système numérique classifié ne peuvent faire l'objet d'un sous-contrat sauf dérogation accordée d'un commun accord par l'autorité contractante et le service enquêteur et inscrite dans le plan contractuel de sécurité.

Lorsque des services ou des infrastructures sont mutualisés et utilisés dans le cadre de plusieurs contrats, l'autorité d'homologation s'assure du respect des règles spécifiques

¹⁹⁹ Au sens de l'article L.2393-7 du code de la commande publique.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.5**

de sécurité liées à ces contrats, le cas échéant, et du bon cloisonnement des informations.

L'emploi d'un service numérique fourni par un tiers pour l'exécution du contrat est soumis à homologation (c'est alors l'emploi qui est fait du service, et non le système numérique qui le fournit et sur lequel l'autorité d'emploi n'a pas autorité, qui est homologué). L'entité propriétaire du système numérique reste responsable du contrôle régulier et indépendant de la mise en œuvre des prestations d'administration de la sécurité. Ces contrôles devront être réalisés conformément aux dispositions relatives aux audits et à la gestion des sous-contractants. Des prestataires qualifiés pourront être sollicités dans le cadre de ces activités.

1. Analyse de risques préalable par l'autorité contractante

Une analyse de risques est nécessaire pour formaliser des objectifs de sécurité ainsi que des mesures adaptées au contexte. Celle-ci permettra à l'autorité d'homologation d'autoriser ou non la sous-contractance.

Le cocontractant doit veiller à conserver la maîtrise du système numérique (gouvernance, dépendance technologique, etc.).

Trois sources principales de risques liées à la démarche de sous-contractance à un tiers doivent être envisagées :

- les interventions à distance (liaisons permanentes avec droits privilégiés, télé-administration de passerelles de sécurité, interconnexions non sécurisées, mots de passe faibles, etc.) ;
- l'externalisation et la mutualisation de l'hébergement (isolation défaillante entre les clients ou avec le fournisseur de service, effacement incomplet ou non sécurisé, etc.) ;
- l'exposition à des réglementations extraterritoriales (exemple : *Cloud Act* adopté en mars 2018 par les États -Unis).

Si la prestation est effectuée à distance, et selon la complexité et les enjeux de sécurité du système numérique, elle pourra être complétée par les documents suivants :

- un document délimitant distinctement les périmètres de responsabilité de chacune des parties, notamment en ce qui concerne le maintien en conformité du service (gestion de la traçabilité, gestion des comptes, MCO/MCS, etc.) et la gestion des informations et supports classifiés ;
- un document de procédures d'exploitation de sécurité, fixant les modalités générales d'exploitation de sécurité des dispositifs de télémaintenance ;
- des fiches réflexes permettant de garantir la bonne application des procédures d'exploitation de sécurité par le personnel en charge de l'utilisation ou de l'administration des dispositifs de télémaintenance.

Si l'analyse de risques fait apparaître un risque pour l'autorité contractante, alors celle-ci doit en être informée.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.5****2. Processus contractuel d'externalisation par le cocontractant de l'administration**

Le contrat de sous-contractance à un tiers comprendra les clauses de sécurité – y compris celles devant s'appliquer aux sous-traitants en cascade – et celles relatives à la réversibilité. Le contrat précisera la possibilité d'effectuer des audits de sécurité à son niveau ou par l'administration. Le périmètre d'intervention du prestataire doit y être établi avec délimitation claire de ses fonctions et responsabilités – notamment en matière de sécurité – vis-à-vis de celles conservées par le donneur d'ordre.

Tout contrat de sous-contractance nécessitant un accès à des informations et supports classifiés ou à un article contrôlé de la sécurité des systèmes d'information (classifié ou non) est soumis à l'autorisation explicite de l'autorité contractante. Ce contrat :

- obéit aux règles de l'IGI 1300 et de l'IM 900 ;
- comporte des clauses de protection du secret (cf. IGI 1300 – annexe 17) ;
- implique l'habilitation préalable des personnes morales et physiques ;
- nécessite les aptitudes physiques des locaux et techniques des systèmes d'information support de la prestation.

Ces contrats impliquant l'accès ou la détention d'informations et supports classifiés ou à des moyens et supports articles contrôlés de la sécurité des systèmes d'information, qu'ils soient classifiés ou non, font alors l'objet d'un plan contractuel de sécurité qui décline les objectifs de confidentialité (fiche 4.8 de la présente instruction).

Toute prestation d'infogérance nécessitant un accès à des informations *Diffusion Restreinte* devra se conformer aux règles du guide de l'ANSSI « Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques », au « Recueil de mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau *Diffusion Restreinte* » et à l'annexe 3 de l'IGI 1300. Il sera porté une attention particulière à la localisation géographique de l'hébergement des données et à l'homologation *Diffusion Restreinte* du système numérique.

Il doit être demandé aux candidats un descriptif des dispositifs de télémaintenance et des mesures techniques et organisationnelles de sécurité proposées :

- la sécurité de la liaison : réseau public ou ligne spécialisée, type de VPN, etc. ;
- les dispositifs techniques de sécurité : filtrage des accès réseau, droits d'accès, etc. ;
- les mesures organisationnelles, les procédures retenues pour déclencher une intervention ;
- les mécanismes d'authentification des techniciens assurant le support ;
- la traçabilité des actions ;
- la protection des accès aux données confidentielles en cas d'utilisation sur un système de production ;
- les éventuels rapports d'audit et plans d'action afférents.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.6****PRISE EN COMPTE DE LA SÉCURITÉ DANS LE CYCLE DE VIE DES SYSTÈMES NUMÉRIQUES****Références :**

- IGI 1300 – 6.6. et 6.6.3.1
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles

Point clé

- La sécurité doit être prise en compte tout au long du cycle de vie d'un système numérique depuis la phase de conception/développement en passant par la phase d'exploitation (maintien en condition opérationnelle et de sécurité) jusqu'au retrait de service. Elle est à la charge de l'autorité qualifiée en sécurité des systèmes d'information du système concerné.

1. Principes

Afin de prévenir les attaques informatiques, les systèmes numériques et les applications « métier » doivent être développés de manière robuste et sécurisée conformément aux objectifs de sécurité issus d'une analyse de risques. La sécurité doit être prise en compte dès la conception d'un système jusqu'à sa fin de service. Cette précaution relève de l'autorité qualifiée en sécurité des systèmes d'information concernée. Le responsable de la sécurité des systèmes d'information du système concerné est chargé d'organiser cette prise en compte.

Les modalités de destruction, d'effacement, de recyclage, etc. des supports de données et des matériels informatiques doivent être anticipées, en particulier pour les informations et supports classifiés et les articles contrôlés de la sécurité des systèmes d'information.

À cet effet, l'ANSSI fournit des guides et recommandations relatifs à l'intégration de la sécurité dans le développement d'un système numérique, la maîtrise des risques « cyber » ou encore la configuration et la sécurité des solutions disponibles sur étagère.

Tout organisme mettant en œuvre un système numérique traitant des informations *Diffusion Restreinte* doit se conformer aux exigences de l'II 901.

Tout organisme mettant en œuvre un système numérique traitant des informations classifiées au niveau *Secret* ou *Très Secret* doit se conformer aux exigences de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

2. Cycle de vie des informations et supports classifiés

Une grande partie des équipements constitutifs des systèmes numériques est équipée de supports physiques de stockage rémanent (mémoires de masse de type disque dur magnétique, SSD, mémoire flash, etc.). On les retrouve au sein d'équipements tels que les serveurs, ordinateurs individuels, robots de sauvegarde, périphériques de stockage,

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.6**

copieurs multifonctions, « ordiphones », vidéoprojecteurs, systèmes de visioconférence, matériels de téléphonie et équipements de réseau.

Sur les systèmes numériques classifiés, ces supports physiques²⁰⁰ contiennent des informations classifiées et doivent être traités, si les informations ne sont pas chiffrées par un dispositif agréé, comme étant des supports classifiés physiques, soit de façon unitaire, soit au niveau de l'équipement.

Les informations et supports classifiés sont marqués, enregistrés et tracés conformément au titre 7 de la présente instruction. À chaque étape de la vie du système, la traçabilité et la gestion réglementaire de ces informations et supports classifiés doivent être assurées.

Les modalités de fin de vie, en particulier, les modalités de destruction des informations et supports classifiés et des articles contrôlés de la sécurité des systèmes d'information du système numérique ou les contraintes et restrictions liées au réemploi des matériels non classifiés doivent être prévues dès le départ.

L'authentification forte est obligatoire pour tout système numérique classifié dont la protection logique doit répondre à une classe α ou β ²⁰¹. Pour les systèmes numériques traitant des informations *Diffusion Restreinte* et sensibles, une authentification forte sera également mise en œuvre. En fonction des besoins déterminés lors de l'analyse de risque, des dérogations à ces règles sont possibles mais doivent être justifiées dans le dossier d'homologation. Les éléments d'authentification associés à leur contexte d'utilisation doivent être considérés comme étant du niveau de sensibilité ou de classification du système numérique auquel ils permettent l'accès.

3. Conception et exploitation du système numérique

L'homologation est un prérequis pour la mise en service d'un système numériques (cf. fiche 6.2).

a. Administration des systèmes numériques

Les actions d'administration permettent de maintenir le système numérique en condition opérationnelle et de sécurité. Qu'il s'agisse d'actions liées à des évolutions du système numérique ou à l'exploitation courante, celles-ci nécessitent des privilèges. Elles constituent à ce titre une activité critique.

Les politiques de sécurité listent les différents types de comptes à privilège et a minima :

- les comptes d'administration système (en particulier les administrateurs des annuaires) ;
- les comptes des administrateurs de sécurité ;
- les comptes des administrateurs du réseau ou des services d'infrastructure (socle de virtualisation, service de nom de domaine, etc.) ;

²⁰⁰ Sauf exception devant faire l'objet d'une preuve formelle dont les modalités sont à valider par l'autorité contractante et le service enquêteur.

²⁰¹ Conformément aux tableaux de combinaison des classes de l'IGI 1300 – Annexe 30 – 2.d et 3.b.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.6**

- les comptes de service.

Dans la mesure du possible, les administrateurs systèmes et réseaux sont distincts des administrateurs de sécurité.

b. Maîtrise des logiciels en exploitation

La surface d'attaque de tous les composants d'un système numérique doit être réduite à son minimum. Cette disposition s'applique à tous les équipements composant le système et à tous leurs services (BIOS, services réseaux, applicatifs métiers, etc.).

Le système numérique utilise des logiciels soutenus par les éditeurs et régulièrement mis à jour.

Les ressources logicielles et matérielles font l'objet d'une procédure de gestion de configuration, définie dans le cadre de l'homologation. Sauf difficulté technique ou opérationnelle justifiée, l'installation des mises à jour de sécurité est planifiée après vérification de l'origine de la version et de son intégrité. Lors d'une décision de ne pas installer la mise à jour, des mesures techniques et organisationnelles sont mises en œuvre pour réduire les risques liés à l'utilisation de cette version obsolète ou vulnérable.

c. Contrôle d'accès aux systèmes classifiés

L'accès aux systèmes d'information doit être restreint et contrôlé, en cohérence avec les principes de moindre privilège et de besoin d'en connaître.

Une personne physique disposant de droits d'accès administrateur d'un système numérique *Secret* ou *Très Secret* doit être habilitée au niveau *Très Secret*.

La nécessité d'habiliter ou non une personne physique disposant de droits d'accès administrateur sur un système numérique *Diffusion Restreinte* est définie dans le PCS par l'autorité contractante.

Une personne physique ne possédant pas de compte administrateur est habilitée au même niveau que le système numérique.

Les exigences ci-dessus concernant le niveau d'habilitation des administrateurs sont sans incidence sur le niveau d'habilitation de la personne morale.

d. Gestion des privilèges

Le principe du « moindre privilège » doit être appliqué. À cet effet, le nombre d'administrateurs sera réduit autant que possible et des revues périodiques des droits seront menées, au moins annuellement.

Les comptes d'administration doivent être attribués individuellement et ne doivent être utilisés qu'à des fins d'administration. L'utilisation du système numérique se fait exclusivement avec des privilèges restreints d'utilisateur.

Les utilisateurs ne doivent pas pouvoir modifier les paramètres de configuration de démarrage de leur poste.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.6****4. Maintien en condition opérationnelle (MCO) et en condition de sécurité (MCS)****a. Généralités**

Les activités de MCO et de MCS assurent le maintien du niveau de fonctionnalité et de sécurité du système numérique, de la conception du système jusqu'à son retrait du service. Elles assurent en particulier que le niveau de sécurité est constant et que les risques restent maîtrisés.

Les processus de MCO, de MCS, incluant les mesures de sécurité mises en œuvre pour encadrer les activités de maintenance, font partie du périmètre d'homologation du système.

b. Exigences particulières liées à la maintenance

Les opérations de maintenance sur un système numérique classifié doivent obligatoirement être tracées et imputées.

Avant chaque intervention de maintenance, il est obligatoire de s'assurer de la mise en place des mesures de préservation des informations à protéger et des équipements classifiés, sensibles ou *Diffusion Restreinte* (une procédure d'effacement pourra être mise en œuvre avant toute intervention de la société de maintenance). L'organisme en charge de la maintenance doit apporter les garanties nécessaires et suffisantes pour attester de l'innocuité des supports physiques et des ressources numériques employées lors de ses interventions.

Après l'intervention, la configuration du système est vérifiée afin de s'assurer de sa conformité avec l'état requis. En particulier, il est vérifié que les modifications apportées n'altèrent pas le niveau de sécurité pour lequel une homologation a été prononcée. Si l'intervention est associée à une évolution significative du système et notamment de sa configuration, elle peut donner lieu à une nouvelle homologation du système (cf. fiche 6.2).

Seuls les composants matériels explicitement autorisés dans le dossier d'homologation du système numérique peuvent être connectés à des systèmes numériques classifiés.

Une personne physique en charge de la maintenance ayant potentiellement accès à des informations classifiées est habilitée au même niveau que le système numérique sur lequel elle est amenée à effectuer une opération de maintenance. Si elle n'est pas habilitée à ce niveau, elle est accompagnée pendant toute l'opération par un agent habilité et ayant des compétences suffisantes pour s'assurer que la personne en charge de la maintenance n'ait pas accès à des informations classifiées et n'introduise pas d'élément non maîtrisé dans le système numérique traitant d'informations classifiées ou n'effectue pas des opérations non prévues dans le cadre de son intervention.

Les contrats d'approvisionnement et de maintenance d'équipements qui intègrent des supports physiques pour traiter des informations classifiées ou *Diffusion Restreinte* doivent comprendre des clauses de non-retour de ces supports chez les fournisseurs, applicables dès lors que ces supports ont traité des informations classifiées ou *Diffusion Restreinte*.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ

6.6**5. Interconnexions**

Le transfert d'informations entre deux réseaux de classifications différentes se fait idéalement par une passerelle agréée par l'ANSSI ou homologuée et prévue à cet effet (généralement équipée d'une ou de plusieurs diodes).

À défaut de la mise en place d'interconnexions avec transfert direct d'informations, le transfert peut être effectué *via* un support amovible exclusivement dédié à cet effet selon une procédure définie et prise en compte dans l'homologation, qui permet notamment de vérifier son innocuité et de maîtriser les supports amovibles utilisés pour de tels transferts.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.7****ÉQUIPEMENTS MOBILES ET SUPPORTS AMOVIBLES****Références :**

- IGI 1300 – 6.7, 6.8 et 7.3.2.2
- II n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles
- Guide ANSSI-PA-054 recommandations sur le nomadisme numérique

Points clés

- Le chiffrement permet d'assurer la protection des informations traitées par des équipements mobiles ou conservés sur des supports amovibles, particulièrement en dehors des locaux protégés. Ce chiffrement doit être qualifié (standard ou renforcé) ou agréé en fonction du niveau de protection des informations.
- Les équipements utilisés et leur configuration doivent être gérés logistiquement et administrés par l'entité conformément aux procédures d'exploitation de la sécurité définies lors de la démarche d'homologation.

1. Généralités

Le traitement d'informations sensibles, *Diffusion Restreinte* ou classifiées en dehors des locaux adaptés nécessite la mise en place de mesures techniques et organisationnelles. Ces mesures doivent protéger l'accès aux données numériques et aux matériels. Ces mesures visent à atteindre un niveau de sécurité conforme à ce qu'il serait en dehors d'une utilisation en mobilité.

Le traitement d'informations classifiées en mobilité est conditionné par la maîtrise de l'environnement devant permettre de garantir la confidentialité des informations. Aussi, un tel traitement est interdit dans un espace ouvert au public (aéroport, train, etc.) ou dans lequel la sécurité n'est pas maîtrisée. L'utilisateur doit empêcher la proximité de personnes n'ayant pas le besoin d'en connaître, et s'assurer de l'absence de moyens de captation de sons et d'images.

Il est recommandé de privilégier le fonctionnement sur batterie et non sur secteur. Par ailleurs, un éloignement d'un mètre des sources de conduction (réseaux électriques, réseaux informatiques ou téléphoniques, etc.) doit être respecté, sauf dérogations prévues par l'autorité d'homologation.

2. Protection des informations contre la perte ou le vol

Dans le cas du transport d'un support amovible (terminal portable, clé USB, etc.) contenant des données sensibles, *Diffusion Restreinte* ou classifiées, les informations doivent être chiffrées avec un produit agréé²⁰².

²⁰² La liste des produits agréés est disponible sur le site de l'ANSSI.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.7**

Par principe de prudence, seules les informations strictement nécessaires à la mission doivent être conservées sur le support amovible.

3. Gestion de la protection des matériels et supports amovibles

Les terminaux et postes de travail utilisables en condition de mobilité, d'une part, et les supports amovibles, d'autre part, doivent être considérés comme étant partie intégrante du ou des systèmes auxquels ils peuvent être connectés. Ils sont inclus dans l'analyse de risques et explicitement autorisés dans le dossier d'homologation. Ces équipements doivent être fournis et administrés par l'organisme.

En dehors des locaux protégés de l'organisme, les terminaux et postes de travail doivent rester sous la surveillance permanente de l'utilisateur.

Lorsqu'elle est prévue par le dossier d'homologation, l'utilisation des terminaux et postes de travail à l'étranger est possible. En plus des restrictions ou autorisations prévues par ces conditions générales, les matériels doivent rester sous la surveillance permanente de l'utilisateur. En amont du déplacement, les utilisateurs doivent recevoir une sensibilisation aux conditions particulières de protection des informations dont ils sont dépositaires (dépôt de ces matériels dans le meuble de sécurité, étiquettes ou enveloppes de sécurité, scellés, etc.).

Un terminal ou un poste de travail utilisé en mobilité pour traiter des informations et supports classifiés doit faire l'objet de vérifications régulières de sa configuration physique, en particulier avant qu'il soit reconnecté sur le système numérique homologué de son organisme d'appartenance.

4. Branchement de supports amovibles sur les systèmes d'information

Les supports amovibles classifiés ne doivent pas être connectés à un équipement de niveau de classification ou de sensibilité inférieur à celui de cet équipement, hormis lors du branchement sur une station blanche ou un système de transfert prévu à cet effet. Les ports USB des systèmes d'information classifiés doivent faire l'objet d'un verrouillage ou d'un contrôle afin de prévenir les extractions non autorisées, tracer l'utilisation des supports externes et éviter les compromissions du fait de mauvaises manipulations.

5. Cas particulier de la mobilité via Internet

Un service de mobilité peut être mis en œuvre entre un utilisateur et son entité d'appartenance *via* Internet (filaire ou sans fil) jusqu'au niveau *Diffusion Restreinte* à la condition de se conformer aux exigences de l'II 901, complétées par les recommandations de l'ANSSI.

Les mesures spécifiques à ce type de mobilité doivent être définies dans la PSSI de l'organisme.

En particulier, il est impératif de :

- homologuer au niveau requis le système numérique utilisé en mobilité via Internet ;
- maîtriser la gestion des utilisateurs et des équipements de mobilité ;
- sensibiliser les utilisateurs sur leurs obligations face aux risques et menaces ;

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.7**

- appliquer des restrictions d'usage (séquence de démarrage, filtrage Internet, désactivation des services et applications inutiles, etc.) afin de réduire la surface d'attaque ;
- mettre à disposition des moyens de protection (chiffrement, filtre écran, scellés, verrous sur les ports USB, etc.) ;
- mettre en œuvre un tunnel VPN adapté ;
- mettre en place une passerelle sécurisée d'interconnexion au système numérique interne ;
- assurer l'authentification forte de l'utilisateur et de l'équipement ;
- assurer le maintien en condition opérationnelle et le maintien en condition de sécurité, la supervision, la journalisation et la détection.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.8****SUPERVISION DE SÉCURITÉ D'UN SYSTÈME NUMÉRIQUE****Références :**

- IGI 1300 – 6.6.4
- II n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles
- Arrêté du 8 septembre 2017 modifié fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Activités industrielles de l'armement » et pris en application des articles R.1332-41-1, R.1332-41-2 et R.1332-41-10 du code de la défense

Point clé

La supervision de sécurité d'un système numérique est un élément clé de la cybersécurité, qu'il soit ou non classifié.

Sauf mention contraire, la présente fiche concerne les systèmes d'information classifiés, tels que décrits dans le chapitre 6 de l'IGI 1300, et *Diffusion Restreinte*, au sens de l'II 901 citée en référence.

1. Journalisation des événements

À des fins d'investigation, de suivi *a posteriori* des échanges, de traitement des incidents et d'archivage, une journalisation des événements est mise en place pour tracer et imputer les actions réalisées sur les systèmes d'information selon les recommandations de l'ANSSI. La journalisation porte sur :

- la gestion des accès ;
- les modifications ;
- les enregistrements ;
- tout élément permettant l'investigation en cas d'incident de sécurité.

Les événements enregistrés par le système de journalisation²⁰³ sont horodatés. Les composantes du système doivent être synchronisées pour assurer un horodatage cohérent des événements enregistrés.

Les données de traçabilité des accès sont archivées pour une durée d'au moins trois ans pour le niveau *Secret* et cinq ans pour le niveau *Très Secret*. Pour les systèmes *Diffusion Restreinte* et sensibles, les événements sont conservés sur douze mois glissants. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.

Dans l'éventualité où, pour un système numérique classifié, certains événements ne pourraient être enregistrés, le dossier d'homologation doit préciser les éventuelles mesures organisationnelles palliatives mises en place.

²⁰³ Le système de journalisation est une fonction indépendante du système numérique, qui enregistre les événements relatifs au fonctionnement du système et à sa gestion.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.8**

L'autorité d'homologation s'assure de la définition de procédures d'exploitation des événements enregistrés par le système de journalisation et de leur application.

2. Systèmes de détection

La supervision de la sécurité des systèmes d'information s'appuie notamment, en complément de la journalisation des événements, sur des systèmes de détection de type « sonde d'analyse de fichiers et de protocoles », qui font l'objet d'une stratégie de déploiement et d'une stratégie d'exploitation approuvées par l'autorité qualifiée en sécurité des systèmes d'information. La stratégie de déploiement s'assure, notamment, que l'ensemble des flux de données échangés avec d'autres systèmes d'information est analysé.

L'architecture de déploiement des systèmes de détection ne doit pas remettre en cause la sécurité du système numérique. Les systèmes de détection journalisent l'ensemble des éléments qu'ils détectent.

Si la mise en œuvre des systèmes de détection de type « sonde d'analyse de fichiers et de protocoles » est impossible pour des raisons techniques ou organisationnelles ou sur le fondement d'une analyse de risques réalisée par le responsable de la sécurité du système numérique dans le cadre de l'homologation, l'autorité d'homologation peut déroger, après accord de l'autorité contractante, à la mise en place d'un système de détection. La justification figure dans le dossier d'homologation.

3. Déclaration des incidents

En cas d'incident détecté, dans le périmètre d'un système numérique soumis à la présente instruction ou sur un système numérique ayant une adhérence ou une proximité avec un tel système numérique²⁰⁴, l'opérateur privé doit le déclarer à l'administration. Une campagne d'appui à la détection de compromission²⁰⁵, voire un audit conseil, peut être initiée par le service enquêteur.

Hors cas particulier (contrôle gouvernemental, si l'autorité contractante est la DGSE, etc.), la déclaration initiale d'incident se fait avec l'usage d'un formulaire unique (formulaire type ANSSI), transmis à :

- pour le SIIV : l'ANSSI, copie DRSD, DGA/SSDI et acteurs complémentaires prévus dans le contrat ;
- pour les autres systèmes numériques : la DRSD et l'autorité contractante, copie DGA/SSDI et acteurs complémentaires prévus dans le contrat.

À la suite d'un incident, la DRSD et la DGA/SSDI²⁰⁶ peuvent mener, en coordination avec l'ANSSI et le COMCYBER, des contrôles sur les systèmes numériques soumis à la présente instruction ainsi que sur les systèmes sensibles ou non protégés qui appartiennent à l'environnement d'un réseau classifié ou *Diffusion Restreinte*.

²⁰⁴ Notamment si la confidentialité, l'intégrité ou la disponibilité peuvent être altérées.

²⁰⁵ Cf. définition au paragraphe 1 de la fiche introductive du titre 8.

²⁰⁶ Ou la DGSE pour son périmètre de compétence.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.9****LES ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ACSSI)****Références :**

- IGI 1300 – 6.6.3.3
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- La qualification d'article contrôlé de la sécurité des systèmes d'information (ACSSI) garantit la traçabilité comptable et géographique de ces éléments contribuant à la sécurité des systèmes numériques.
- La qualification comme article contrôlé de la sécurité des systèmes d'information ne préjuge pas de la classification de cet objet (qui peut être aussi NP ou DR).
- Pour manipuler des articles contrôlés de la sécurité des systèmes d'information, une décision d'accès est nécessaire (DACSSI). Elle est délivrée après une formation spécifique.

1. Définitions

Au titre de la présente instruction, le ministère de la défense considère que les articles contrôlés de la sécurité des systèmes d'information (ACSSI) sont des **moyens et supports d'information physiques** qu'il est nécessaire de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée (perte ou incident de sécurité remettant en cause l'intégrité, la confidentialité, la disponibilité ou l'authenticité de l'article).

La décision de classer comme article contrôlé de la sécurité des systèmes d'information un moyen est prise par l'ANSSI après avis de la commission d'agrément du dispositif de sécurité concerné. Dans le cas où le dispositif de sécurité n'est pas soumis à agrément, l'autorité d'homologation d'un système numérique qui met en œuvre un tel dispositif de sécurité peut décider, après avis de la commission d'homologation, de classer comme article contrôlé de la sécurité des systèmes d'information ce dispositif ou les composants qui y sont liés. L'autorité contractante peut également attribuer le statut d'ACSSI à des composants développés ou utilisés dans le cadre de l'exécution du contrat.

La qualification d'article contrôlé de la sécurité des systèmes d'information et leur classification procèdent de deux logiques différentes. La qualification d'article contrôlé de la sécurité des systèmes d'information vise à apporter une assurance de traçabilité (la localisation doit être connue à tout moment) et d'intégrité, la protection physique, logique et juridique de l'article contrôlé de la sécurité des systèmes d'information étant apportée par son niveau de classification. Ainsi, les articles contrôlés de la sécurité des systèmes d'information classifiés sont à la fois articles contrôlés de la sécurité des systèmes d'information et classifiés *Secret* (ACSSI S) ou *Très Secret* (ACSSI TS). Les

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ

6.9

articles contrôlés de la sécurité des systèmes d'information non classifiés sont *Diffusion Restreinte* (ACSSI DR) ou *Non protégé* (ACSSI NP).

2. Règles générales

La décision d'agrément du dispositif de sécurité ou la décision d'homologation peut inclure des règles ou des dérogations spécifiques.

Les articles contrôlés de la sécurité des systèmes d'information portent un marquage spécifique identifiant, en plus, le cas échéant, leur mention de classification. Le marquage est définitif jusqu'à la destruction du dispositif (ou éventuellement la décision de retirer le marquage « article contrôlé de la sécurité des systèmes d'information » par l'autorité qui en avait décidé le marquage).

Certains articles utilisés dans le cadre de l'OTAN et de l'UE, ou d'autres partenariats internationaux, sont assimilés et gérés comme des articles contrôlés de la sécurité des systèmes d'information sur le territoire national, notamment les articles portant la mention CCI (Controlled COMSEC/Cryptographic Item) ou CRYPTO.

Stockage : les articles contrôlés de la sécurité des systèmes d'information classifiés sont conservés comme des informations et supports classifiés de même niveau de classification²⁰⁷. Les articles contrôlés de la sécurité des systèmes d'information non classifiés sont conservés dans des armoires ou des locaux fermés à clé afin de garantir en permanence leur intégrité.

Utilisation : les articles contrôlés de la sécurité des systèmes d'information doivent être manipulés et protégés conformément aux modalités applicables au niveau de classification des informations qu'ils protègent.

Maintenance : les opérations de maintenance d'un article contrôlé de la sécurité des systèmes d'information doivent être soigneusement tracées. Elles font partie intégrante de l'historique de l'article contrôlé de la sécurité des systèmes d'information.

Destruction : les conditions de destruction des articles contrôlés de la sécurité des systèmes d'information sont définies par l'agrément ou la décision d'homologation. Par défaut, ce sont celles définies par l'IGI 1300 et l'II 910. Leur destruction (ou le cas échéant la restitution) doit être prévue dès leur achat afin de garantir que la personne morale dispose des moyens ou soit en mesure de faire appel aux services nécessaires.

L'accès à un article contrôlé de la sécurité des systèmes d'information nécessite une décision d'accès aux articles contrôlés de la sécurité des systèmes d'information (DACSSI). Pour les industriels de la défense, hors contractants avec la DGSE, elle est délivrée après une formation reconnue par l'autorité d'habilitation de la personne morale.

Le prêt ou la mise à disposition de moyens et supports marqués articles contrôlés de la sécurité des systèmes d'information ne peut être effectué que dans le cadre d'une convention ou d'un contrat liant les parties ou d'un marché comportant un plan contractuel de sécurité dont les plans de transports envisagés. La convention ou le

²⁰⁷ Lorsque des articles contrôlés de la sécurité des systèmes d'information sont conservés dans le même meuble que des informations et supports classifiés, ils doivent être spécifiquement marqués de façon à être immédiatement visibles par l'utilisateur.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.9**

marché précise obligatoirement les modalités de restitution et de destruction des articles contrôlés de la sécurité des systèmes d'information concernés.

Transport physique d'articles contrôlés de la sécurité des systèmes d'information classifiés :

- il est réalisé selon les mêmes conditions que le transport d'informations et supports classifiés de même niveau de classification. Vers l'étranger, le convoyeur dispose d'un certificat de courrier²⁰⁸.

Transport physique d'articles contrôlés de la sécurité des systèmes d'information non classifiés : catégorie d'équipements de cryptographie :

- il est réalisé selon les règles applicables au niveau Secret ;
- vers l'étranger, le convoyeur dispose d'un certificat de courrier.

Transport physique d'articles contrôlés de la sécurité des systèmes d'information non classifiés hors équipement cryptographique :

- il est réalisé selon les règles applicables au *Diffusion Restreinte* ;
- l'article contrôlé de la sécurité des systèmes d'information est mis sous double enveloppe (si ses dimensions le permettent).

Dans tous les cas :

- les convoyeurs ne sont pas tenus d'avoir une décision d'accès aux articles contrôlés de la sécurité des systèmes d'information²⁰⁹ ;
- le transport d'un article contrôlé de la sécurité des systèmes d'information donne lieu à un bordereau ABB' permettant de s'assurer de la bonne réception de l'article contrôlé de la sécurité des systèmes d'information et de son intégrité ;
- le plan contractuel de sécurité, la convention ou la décision d'agrément peut générer des obligations complémentaires ;
- pour les articles contrôlés de la sécurité des systèmes d'information non classifiés, l'emploi de conteneurs sécurisés homologués par l'État est possible afin de s'affranchir d'une surveillance permanente, sous réserve de respecter la procédure en vigueur au sein du ministère de la défense telle que précisée dans le plan contractuel de sécurité ou la convention ou disponibles auprès du Commandement des réseaux particuliers de l'armement (CRPA).

3. Responsabilité et gestion des articles contrôlés de la sécurité des systèmes d'information

Les articles contrôlés de la sécurité des systèmes d'information sont suivis de manière centralisée par défaut. Les articles contrôlés de la sécurité des systèmes d'information non classifiés, sous réserve que l'agrément ne l'interdise pas, peuvent être suivis en gestion locale sur décision de l'autorité qualifiée en sécurité des systèmes d'information concernée. Cependant, l'échelon central doit pouvoir accéder à leurs informations de suivi pour fournir, autant que de besoin, une vision globale à la DGA. Afin d'assurer le

²⁰⁸ Conformément aux dispositions relatives au transport des informations et supports classifiés du titre 7.8.

²⁰⁹ Sous réserve que leur emploi ne nécessite pas de manutention d'ACSSI non colisés.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.9**

suivi et la traçabilité des articles contrôlés de la sécurité des systèmes d'information, l'autorité qualifiée en sécurité des systèmes d'information d'une personne morale de droit privé doit désigner un gestionnaire central unique (ou un officier central chiffre) au sein de la chaîne de sécurité numérique. Ce dernier dirige la gestion centralisée des articles contrôlés de la sécurité des systèmes d'information et la sécurité des réseaux de chiffrement associés. La base centralisée de données de gestion du chiffre est classifiée au minimum *Secret*.

Les personnes morales de droit privé sont responsables, sous le contrôle de la DGA, de la mise en œuvre des procédures réglementaires prescrites par la présente instruction pour la gestion des articles contrôlés de la sécurité des systèmes d'information. Elles doivent être en mesure de fournir à la DGA/CRPA et au fonctionnaire de sécurité des systèmes d'information autant que de besoin, une vision globale des articles contrôlés de la sécurité des systèmes d'information qu'elles détiennent. Un inventaire annuel des articles contrôlés de la sécurité des systèmes d'information qu'elles acquièrent ou détiennent en compte d'emploi doit être adressé à la DGA/CRPA qui les communique au fonctionnaire de sécurité des systèmes d'information.

Le suivi d'un article contrôlé de la sécurité des systèmes d'information consiste à :

- pouvoir déterminer la position géographique d'un article contrôlé de la sécurité des systèmes d'information à tout instant ;
- pouvoir déterminer l'exploitant, l'utilisateur, le comptable ou le gestionnaire d'un article contrôlé de la sécurité des systèmes d'information à tout instant ;
- pouvoir déterminer l'état ou le statut d'un article contrôlé de la sécurité des systèmes d'information, pour en particulier distinguer ceux en exploitation de ceux stockés.

Des inspections programmées ou inopinées sont menées par ou pour le compte de la DGA. Elles visent à s'assurer de la bonne tenue, de l'efficacité du suivi spécifique et du respect des mesures de protection. Ces inspections donnent lieu à un procès-verbal suivi de l'élaboration d'un plan d'actions par la personne morale contrôlée, dont l'avancement fait l'objet d'un bilan annuel adressé à la DGA.

4. La gestion des incidents de sécurité

Un incident de sécurité concernant un article contrôlé de la sécurité des systèmes d'information est un événement indésirable ou inattendu présentant une probabilité forte de porter atteinte à la confidentialité, l'intégrité ou la disponibilité des informations ou des systèmes protégés par les articles contrôlés de la sécurité des systèmes d'information. La perte (même temporaire) ou le vol d'un article contrôlé de la sécurité des systèmes d'information, le blocage ou le dysfonctionnement d'un équipement cryptographique article contrôlé de la sécurité des systèmes d'information, le constat d'un défaut d'intégrité d'un article contrôlé de la sécurité des systèmes d'information constituent des catégories d'incidents de sécurité.

Tout incident de sécurité affectant un article contrôlé de la sécurité des systèmes d'information doit faire l'objet d'un compte-rendu immédiat via la chaîne de sécurité numérique. Un inventaire des incidents sera adressé annuellement, par la personne

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.9**

morale à la DGA/CRPA (même en cas d'état néant), qui retransmet une synthèse des informations reçues au fonctionnaire de sécurité des systèmes d'information.

Tout incident de sécurité doit conduire à la mise en œuvre des mesures techniques et organisationnelles, qu'elles soient immédiates (exemple : révocation d'une clé) ou qu'elles soient le fruit d'une analyse par la chaîne des articles contrôlés de la sécurité des systèmes d'information, le fonctionnaire de sécurité des systèmes d'information, le haut fonctionnaire correspondant de défense et de sécurité ou l'ANSSI.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ**6.10****SÉCURITÉ DU CÂBLAGE ET CIRCUITS APPROUVÉS****Référence :**

- IGI 1300 – 6.4.1
- Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 sur la protection contre les signaux parasites compromettants

Point clé

Sous réserve de conditions techniques et d'environnement, les circuits approuvés permettent de faire circuler de façon permanente et en clair des informations classifiées tout en assurant leur protection.

L'installation du câblage d'un réseau transportant des informations classifiées respecte les exigences de la réglementation relative à la protection contre les signaux parasites compromettants.

Le câblage véhiculant en clair des informations classifiées est confiné à l'intérieur de l'environnement de sécurité local et, *a minima*, selon les dispositions prévues par le titre 5 de la présente instruction. Il permet de constituer des réseaux physiquement dissociés et autorise le contrôle de l'infrastructure de câblage.

Pour un système numérique homologué au niveau *Secret*, dans le cas où l'autorité d'homologation prend la responsabilité d'utiliser des circuits approuvés²¹⁰ entre différents environnements de sécurité locaux implantés au sein de la même emprise physique, en remplacement de la mise en œuvre de moyens de chiffrement agréés, une cartographie précise du câblage est détenue par l'officier de sécurité des systèmes d'information et l'officier de sécurité. Le câblage de chaque circuit approuvé doit pouvoir être contrôlé. Les locaux, volumes ou cheminements doivent être protégés soit physiquement, soit par un système d'alarme, soit par un dispositif permettant de vérifier l'intégrité du circuit approuvé, comme de la réflectométrie. En complément de ces dispositions, les informations *Spécial France* ne peuvent circuler sans chiffrement que dans le cas où le circuit approuvé est sous maîtrise et utilisation nationale. Des procédures spécifiques d'exploitation de la sécurité sont établies (contrôles d'intégrité du câblage, etc.).

Il est de la responsabilité de l'autorité qualifiée :

- d'inspecter régulièrement les moyens de protection physique ;
- d'assurer la mise en œuvre des systèmes d'alarme ;
- de contrôler l'intégrité de l'infrastructure de câblage ;
- de s'assurer que les interventions sont effectuées par du personnel habilité (ou accompagné par des agents habilités).

²¹⁰ Un circuit approuvé est un circuit qui fait l'objet de mesures spécifiques de protection physique et visuelle afin de permettre son emploi pour la transmission d'informations classifiées de défense sans protection par des moyens de chiffrement agréés.

TITRE 6 : SÉCURITÉ NUMÉRIQUE POUR LES PERSONNES MORALES DE DROIT PRIVÉ

6.10

L'utilisation d'un circuit approuvé doit faire l'objet de l'accord de l'autorité contractante. Les éléments relatifs au circuit approuvé (cartographie, mesures de sécurité, procédures d'exploitation, etc.) sont pris en compte dans l'analyse des risques et intégrés dans le dossier d'homologation. Ils sont en outre transmis à l'autorité contractante sur simple demande.

Pour un système numérique homologué au niveau *Très Secret*, l'usage de circuits approuvés est interdit, le câblage véhiculant en clair des informations classifiées *Très Secret* est confiné à l'intérieur de la zone réservée.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET DES DONNÉES TOUT AU LONG DE LEUR CYCLE DE VIE

INTRODUCTION : PRINCIPES ET DÉFINITIONS

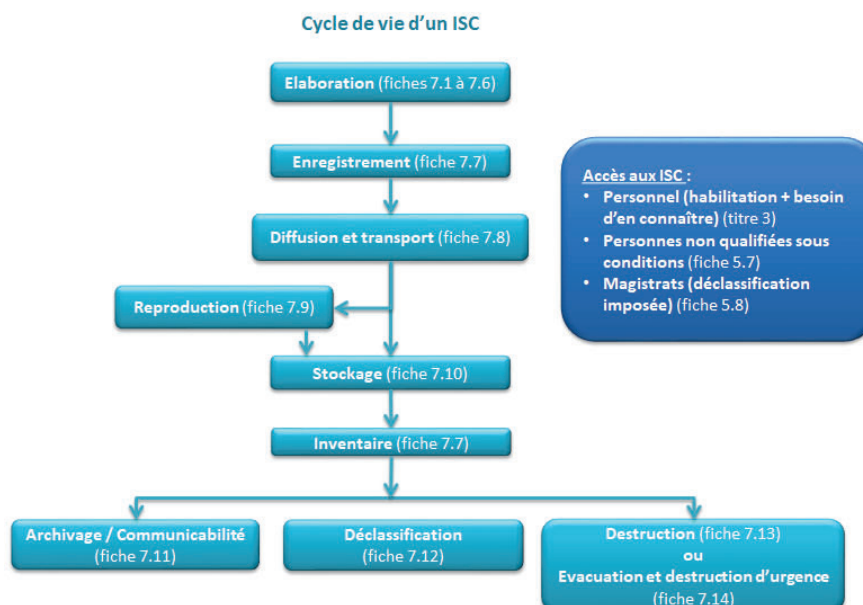
Références :

- Code de la défense – articles R.2311-1 à R.2311-9
- Code pénal – articles 413-9 et suivants
- IGI 1300 – Introduction, chapitres 1 et 7

Points clés

- La défense et la sécurité nationale doivent être les seuls motifs présidant à la décision de classification.
- Classifier un document ou un support lui offre une protection pénale.
- Il existe deux niveaux de classification : *Secret* et *Très Secret*. Des classifications spéciales viennent compléter le niveau *Très Secret* ; leur traitement fait l'objet d'instructions particulières relevant du SGDSN.
- Les informations et supports classifiés avant le 1^{er} juillet 2021 conservent leur marquage d'origine (CD, SD) et la protection juridique afférente. Les règles applicables au niveau *Secret* décrites dans la présente instruction s'appliquent également aux informations et supports classifiés de niveau *Confidentiel Défense* et celles applicables au niveau *Très Secret* s'appliquent aux informations et supports classifiés de niveau *Secret Défense*.

1. Principes



TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

La protection du secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation en empêchant la divulgation, intentionnelle ou non, d'informations pouvant leur porter atteinte ou ayant des conséquences exceptionnellement graves pour eux.

La classification d'une information place celle-ci sous la protection de dispositions spécifiques du code pénal. Cette protection comprend des autorisations nécessaires pour accéder à cette information, des mesures physiques pour en limiter l'accès et des modalités de gestion particulières (enregistrement, inventaire, déclassification, destruction, etc.).

Les différents niveaux de classification correspondent à des mesures de protection plus ou moins renforcées et adaptées au risque encouru en cas de compromission du secret de la défense nationale.

La classification peut être augmentée (reclassement), réduite (déclassement) ou supprimée (déclassification), à l'échéance obligatoirement indiquée sur le document ou à l'échéance de la durée maximale de classification (préalablement officiellement établie ou sur décision particulière).

Les mesures à mettre en œuvre concernant la classification et le suivi des informations et supports classifiés sont décrites dans les fiches 7.1 à 7.14.

Les locaux, les meubles et les systèmes numériques contenant des informations et supports classifiés doivent respecter des normes de protection particulières et adaptées (cf. fiches du titre 5 jusqu'à 5.5).

Toute personne visant ou occupant un poste pour lequel le besoin d'une habilitation est avéré et qui refuserait de se soumettre à la procédure d'habilitation ne peut exercer les fonctions prévues et est écartée (cf. fiche 3.1 et suivantes).

Dans le cadre des marchés, le besoin d'en connaître est défini dans le plan contractuel de sécurité suivant les prescriptions des fiches 4.3 et 4.4.

2. Définitions et champs d'application

Informations et supports classifiés : information, document, support, matériel, procédé, réseau informatique, donnée informatisée ou fichier, quel qu'en soit la forme, la nature ou le mode de transmission, qu'il soit élaboré ou en cours d'élaboration, auquel un niveau de classification a été attribué et qui, dans l'intérêt de la défense nationale et conformément aux procédures, lois et règlements en vigueur, nécessite une protection contre toute violation, toute destruction, tout détournement, toute divulgation, toute perte ou tout accès par toute personne non autorisée ou tout autre type de compromission. Pour avoir accès aux informations et supports classifiés, il faut être habilité et avoir le besoin d'en connaître (cf. IGI 1300 – 3.1.1).

Secret : réservé aux informations et supports dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale ;

Très Secret : réservé aux informations et supports dont la divulgation ou auxquels l'accès aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale. Des classifications spéciales sont créées par le Premier ministre, pour

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

le niveau *Très Secret*, pour protéger les informations relatives aux priorités gouvernementales en matière de défense et de sécurité nationale (cf. fiche 7.6).

Les états-majors, directions et services émetteurs des mentions particulières doivent préciser les règles de gestion des informations et supports classifiés dans une directive dont elles doivent rendre destinataire la chaîne de protection du secret et le bureau de protection du secret des organismes, sauf mesure différente fixée par le ministre de la défense. La chaîne de protection du secret est partie prenante dans la gestion des informations et supports classifiés.

3. Correspondance des niveaux de classification pour les informations et supports classifiés avant le 1^{er} juillet 2021 (date d'entrée en vigueur de l'IGI 1300 édition 2020)

Niveau *Confidentiel Défense* : tout information ou support classifié marqué *Confidentiel Défense* conserve son marquage et la protection juridique associée. Il est traité et protégé selon les mesures de protection applicables aux informations et supports classifiés au niveau *Secret*.

Niveau *Secret Défense* : tout information ou support classifié marqué *Secret Défense* conserve son marquage et la protection juridique associée. Il est traité et protégé selon les mesures de protection applicables aux informations et supports classifiés au niveau *Très Secret*.

L'équivalence des niveaux de classification français avec ceux des autres États est validée avec les Autorités Nationales de Sécurité des pays partenaires ou selon des modalités définies par elles.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.1

ÉLABORATION D'INFORMATIONS ET SUPPORTS CLASSIFIÉS

Références :

- Code pénal – articles 413-9 et suivants
- IGI 1300 – 7.1, annexes 36 à 38
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Les règles d'élaboration et de marquage des informations et supports classifiés permettent d'assurer leur identification et de leur apporter une protection pénale.
- En raison de la possibilité technique de faire réapparaître des informations en principe effacées, un support informatique contenant des informations classifiées conserve toujours le niveau de classification des informations qu'il détient ou qu'il a détenues, sauf si celles-ci ont toutes été déclassifiées préalablement.
- **Il convient de ne classifier uniquement que ce qui est nécessaire en se référant aux guides de classification.**

1. Décision de classifier

Le ministre, en tant qu'autorité émettrice, énonce les critères de classification. Il veille à ce que le niveau de classification soit approprié à l'information ou au support concerné, c'est-à-dire à ce qu'il soit à la fois nécessaire et suffisant. Il cherche ainsi à limiter la prolifération de documents classifiés, à éviter les classifications abusives ou, à l'inverse, les sous-classifications (cf. guide de classification en [annexe 13](#)). Pour le département ministériel, chaque état-major, direction ou service rédige une instruction précisant le guide de classification cité *supra*. Il précise les consignes de déclassification à appliquer aux informations et supports classifiés.

L'auteur d'une information ou d'un support classifié est celui qui prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu, conformément aux modalités de classification arrêtées par l'autorité émettrice. Il procède à l'analyse de l'importance de l'information au regard de son contexte et eu égard aux directives de classification applicables.

2. Élaboration

L'élaboration d'informations et supports classifiés consiste à apposer un timbre de classification visible. Cette classification a pour conséquence de le placer sous la protection des dispositions spécifiques du code pénal²¹¹.

Chaque information et support classifié est obligatoirement élaboré par une personne détenant une habilitation de niveau au moins équivalent à celui de l'information ou du document considéré. Le système numérique servant à l'élaboration des documents ou

²¹¹ Articles 413-9 et suivants du code pénal.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.1

fichiers classifiés fait l'objet d'une homologation au minimum du niveau de classification de l'information concernée. Des informations et supports classifiés peuvent être créés sur un poste isolé, hors réseaux, sous réserve de l'autorisation du chef d'organisme après avoir pris connaissance des risques associés.

L'élaboration d'informations et supports classifiés de niveau *Très Secret* se fait impérativement en zone réservée (cf. fiche 5.2). Il est recommandé d'élaborer des informations et supports classifiés de niveau *Secret* au sein d'une zone protégée (cf. IGI 1300 – 5.3.1.1).

3. Règles de gestion des supports

- Classification de l'objet du document : par principe, l'objet d'un document classifié est lui-même classifié au même niveau que le document sauf si son auteur en décide autrement.
- Les agrégats : un ensemble d'informations ou supports, dit parfois agrégat, est classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ses éléments, pris isolément n'est classifié. Un agrégat d'informations et supports classifiés peut également être classifié à un niveau supérieur à celui des informations et supports classifiés qu'il contient.

Tout agrégat (pages, paragraphes, annexes, appendices, pièces jointes) contenant des informations classifiées à des niveaux différents est classifié lui-même au niveau le plus élevé des informations qu'il contient.

- Les documents composites : lorsqu'un document comprend diverses parties, les unes nécessitant une classification, les autres non, il convient de s'efforcer de préciser le niveau de classification en marge face aux parties ou paragraphes qu'il couvre (cf. modèle dans IGI 1300 annexe 36). Cela revient à marquer entre crochets en tête de paragraphe le niveau de protection de l'information²¹² :

« [S-SF] texte du paragraphe.

[NP] texte du paragraphe. »

Si une partie complète du document présente un niveau de protection homogène alors la mention de protection est située au début du titre de la partie :

« [S-SF] texte du titre.

Texte des paragraphes. »

Pour faciliter la manipulation de ces documents, le bon sens recommande, lorsque cela est possible, d'isoler sur des pages particulières les informations d'un même niveau.

La diffusion des paragraphes non classifiés ou des paragraphes d'un niveau de classification inférieur est rendue possible par extraction des éléments non classifiés ou en rendant illisibles, de manière irréversible, les paragraphes classifiés ou classifiés au niveau supérieur.

²¹² En l'absence de ce marquage, l'information est considérée classifiée au niveau du document. En particulier, en l'absence de ce marquage, l'objet d'un document classifié est lui-même réputé classifié au même niveau que le document.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.1

Le niveau de classification des informations (notices, plans, etc.) concernant un matériel peut être différent du niveau de classification de ce dernier.

Un extrait d'information classifiée conserve le niveau de classification de l'information elle-même, à moins que le responsable d'organisme de l'auteur du document n'en décide autrement. En l'absence d'indication contraire, la diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite. Lorsque des extraits de documents contenant des informations classifiées sont transférés sur un autre support, si ces extraits sont eux-mêmes classifiés, la mention de classification est reportée sur le nouveau support conformément aux dispositions de la présente instruction.

- Les supports préparatoires : les supports préparatoires ayant servi à l'élaboration du document classifié (brouillons, impressions sur papier, matériels informatiques nomades : clés USB, disquettes, CD, CD-ROM, etc.) doivent porter la mention du niveau de classification adapté, ils sont placés sous la responsabilité de celui qui les a élaborés ou modifiés. Ils doivent être détruits ou effacés selon les conditions décrites dans la fiche 7.13 le plus rapidement possible dès qu'ils sont devenus sans objet et en tout état de cause, au plus tard lorsque le document classifié est émis.

4. Marquage

Une information doit pouvoir être identifiée comme étant classifiée avant sa consultation. L'apposition d'un timbre de classification visible constitue le seul moyen de conférer la protection des dispositions spécifiques du code pénal. Le marquage constitue une marque de l'autorité publique permettant de vérifier l'authenticité du support.

Le marquage comprend à la fois le timbre, l'identification et la pagination.

a. Timbre

Il indique le niveau de classification et permet par sa position, sa taille et sa couleur, d'attirer immédiatement l'attention sur le caractère secret de l'information ou du support (cf. modèles en annexe 37 de l'IGI 1300).

Il est apposé, avec une encre de couleur rouge, ou, à titre exceptionnel, d'une couleur contrastant avec celle du support, au milieu du haut et du bas de chaque page. Pour les documents reliés, un timbre d'un modèle de dimension supérieure est placé au milieu du bas de la couverture et de la page de garde (cf. annexe 37 de l'IGI 1300). Le timbre, dont la dimension peut être adaptée à celle du support, est définitif et toujours visible.

Si l'information doit être divulguée aux seuls ressortissants français, le timbre *Spécial France*, de couleur bleue, est apposé sous le timbre de classification de l'information en page de garde ou directement à droite du timbre.

Les abréviations indiquant la classification ou le niveau de protection ainsi que les mentions complémentaires peuvent être utilisées pour préciser le niveau de classification de l'objet et des paragraphes du texte. Les abréviations sont les suivantes :

- *Non protégé* : NP ;
- *Diffusion Restreinte* : DR ;
- *Secret* : S ;

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.1

- *Très Secret* : TS ;
- *Spécial France* : SF.

Ces abréviations ne remplacent pas la mention de classification inscrite en toutes lettres sur le document papier ou dématérialisé.

b. Identification

Tout document classifié est identifié dès sa première page. En plus des références ordinaires de toute pièce administrative, des mesures particulières sont prises. Ainsi, sur la première page du document, figurent :

- le timbre du niveau de classification (cf. annexe 37 de l'IGI 1300) ;
- l'échéance de la classification. Le cas échéant, la mention de déclassé ou de déclassification est apposée sur cette même page (cf. annexe 37 de l'IGI 1300) ;
- les références de l'autorité émettrice et de l'auteur de l'information ou du support classifié ;
- la date d'émission ;
- le numéro d'enregistrement ;
- le niveau de protection ou de classification de l'objet.

Les paragraphes, alinéas, annexes traitant d'informations et supports classifiés à un niveau inférieur ou non classifiés, sont mis en évidence s'il y a lieu, par la mention, dans la marge, de leur propre niveau de classification ou de protection, ou par une mise en page qui les détache sans ambiguïté du contexte général du document.

Au niveau *Très Secret*, chaque document est individualisé par son numéro d'exemplaire et le nombre total d'exemplaires est porté sur la première page. Chaque page porte également la référence du document.

c. Pagination

Chaque page du document est numérotée. Sur la première page sont précisés le nombre total de pages et les annexes ou plans qui le composent.

Les pages de chaque annexe sont numérotées indépendamment de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe sur la première page de celle-ci.

Pour les documents classifiés au niveau *Très Secret*, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention "PAS DE TEXTE".

Marquage d'un support immatériel, d'éléments constitutifs d'un système numérique classifié ou de supports de stockage amovibles

Dans la mesure du possible, les règles de marquage d'un support immatériel doivent respecter les règles de marquage d'un support papier.

Le marquage d'un support immatériel d'information classifiée (message ou fichier électronique, base de données, etc.), des éléments constitutifs d'un système numérique

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.1**

classifié²¹³ ou d'un support de stockage amovible d'informations classifiées est adapté au type de support et est toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle du support. Il peut contenir la mention *Spécial France* si l'information ne peut être divulguée qu'aux seuls ressortissants français ;
- une identification assurée par l'inscription des références et, le cas échéant, du volume de chacune des informations enregistrées.

S'il est matériellement impossible d'apposer le marquage sur le support classifié ou contenant une information classifiée, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation ou la documentation utilisateur. Pour les supports de stockage amovibles agréés, le marquage doit être réalisé dans les conditions prévues par les instructions d'emploi du support, mentionnées dans sa décision d'agrément.

²¹³ Tout périphérique d'entrée non doté d'un élément mémorisant ou de communication sans fil peut être exempté de marquage (ex. claviers, souris, etc.). Cette exemption doit être mentionnée dans le dossier d'homologation.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.2****MENTION DE PROTECTION *DIFFUSION RESTREINTE*****Références :**

- Code des relations entre le public et l'administration (Livre III)
- IGI 1300 – 1.3.2
- Instruction ministérielle n° 26209/ARM/SGA/DAJ du 16 août 2017 relative à la communication par les services du ministère des armées des documents administratifs aux citoyens

Points clés

- En France, la mention *Diffusion Restreinte* (DR) n'est pas un niveau de classification mais une mention de protection apposée par une autorité ministérielle.
- Cette mention ne confère pas aux informations concernées la protection pénale propre au secret de la défense nationale, mais leur divulgation au public est considérée comme un manquement à la discrétion professionnelle voire une atteinte au secret professionnel pouvant faire l'objet d'une peine maximale d'un an de prison et 15 000 € d'amende²¹⁴.
- Le personnel ne respectant pas les règles de discrétion pour cette mention de protection peut faire l'objet d'une sanction administrative, voire pénale²¹⁵.
- La mention *Diffusion Restreinte* ne fait pas obstacle à elle seule à la communication d'un document administratif à une personne qui en ferait la demande au titre du droit d'accès consacré par le livre III du code des relations entre le public et l'administration (Cf. fiche 7.12 sur les conditions particulières de communicabilité).

La mention *Diffusion Restreinte* indique que l'information – bien que non classifiée – ne doit pas être rendue publique et ne doit être communiquée qu'aux personnes ayant besoin de la connaître dans l'exercice de leur fonction ou dans l'accomplissement de leur mission. Cette mention n'est pas, pour la France, un niveau de classification mais une mention de protection. Son objectif principal est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

1. Teneur des informations *Diffusion Restreinte*

Au sein du ministère, l'utilisation de cette mention relève de la nécessité d'éviter la divulgation d'informations dont le regroupement ou l'exploitation peuvent :

- permettre la découverte d'un secret de la défense nationale ou compromettre la protection et la sécurité de la défense ;
- porter atteinte à la sécurité ou à l'ordre public, au renom des armées, à la vie privée de ses ressortissants ;

²¹⁴ Article 226-13 du code pénal.

²¹⁵ Abus de confiance, violation du secret professionnel ou de non-respect des règles relatives au traitement des données à caractère personnel.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.2**

- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics du fait de leurs activités à caractère militaire.

Doivent notamment recevoir au minimum la mention *Diffusion Restreinte* les informations et documents :

- définissant, en termes généraux, les objectifs, options, critères de choix retenus dans les différents domaines de l'activité militaire française, opérationnelle ou technique ;
- relatifs à l'ordre public (comptes rendus d'événements, etc.) ;
- couverts par cette mention en raison d'un accord de sécurité conclu avec un pays étranger ;
- relatifs à des exercices dont la sensibilité défense n'a qu'un intérêt limité et temporaire ;
- émanant d'un autre ministère dont la diffusion n'est pas jugée souhaitable par ce ministère.

Bien que la mention *Diffusion Restreinte* ne soit pas destinée à protéger des informations à caractère personnel, son utilisation reste possible dans le cas de rapports sur le moral ou de comptes rendus d'événements, etc.

2. Autorités habilitées à décider de l'emploi de la mention *Diffusion Restreinte*

Sous l'autorité du ministère, sont autorisés à apposer sur des informations et supports la mention *Diffusion Restreinte* et à y accéder :

- des états-majors, directions et services ;
- des établissements publics placés sous sa tutelle ;
- des opérateurs d'importance vitale relevant des DNS AME et ID.
- des personnes morales, publiques ou privées, avec lesquelles il a conclu une convention, un contrat de commande publique ou un contrat de subvention ainsi que les sous-traitants ou sous-contractants de ces personnes morales ayant également besoin d'accéder à des informations ou supports protégés par la mention *Diffusion Restreinte* pour l'exécution de travaux réalisés en appui du contrat principal.

Tout signataire d'un document contenant des informations répondant aux critères précisés ci-dessus est responsable de l'attribution de la mention *Diffusion Restreinte*.

Il est recommandé de faire signer aux personnes susceptibles d'avoir accès à des informations *Diffusion Restreinte* un engagement de non-divulgence (cf. [annexe 14](#)).

Les informations *Diffusion Restreinte* du ministère de la défense ne doivent être communiquées qu'aux personnes qui ont le besoin d'en connaître.

Une divulgation de ces informations au-delà de ce cercle est considérée comme un manquement à la discrétion professionnelle et peut entraîner des sanctions disciplinaires ou professionnelles pour le personnel l'ayant causée (cf. fiche 3.10).

Toutefois, la mention *Diffusion Restreinte* ne fait pas obstacle à elle-seule à la communication d'un document administratif à une personne qui en ferait la demande au titre du droit d'accès institué par le livre III du code des relations entre le public et l'administration, sous réserve que leur communication ne porte pas atteinte à l'un des secrets protégés par les articles L.311-5 (par exemple la conduite de la politique

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.2

extérieure de la France, la sûreté de l'État, la sécurité publique, la sécurité des personnes ou la sécurité des systèmes d'information des administrations) et L.311-6 du même code (par exemple la protection de la vie privée, le secret médical ou le secret des affaires)²¹⁶.

3. Élaboration et marquage

L'élaboration des documents *Diffusion Restreinte* ne peut être effectuée que dans les lieux offrant des conditions de sécurité suffisantes interdisant l'accès de personnes non autorisées à ces documents.

Les documents et supports *Diffusion Restreinte* doivent être identifiés sur la première page avec les références de l'organisme émetteur, la date d'émission et le numéro d'enregistrement.

Ils portent le marquage suivant :

DIFFUSION RESTREINTE

- sur chaque page, le timbre *Diffusion Restreinte* apposé avec de l'encre de couleur rouge, au milieu du haut de la page (cf. IGI 1300 - annexe 1) ;
- pour les messages et autres documents informatiques, la mention *Diffusion Restreinte* doit être rappelée en début de chaque page ;
- pour les documents reliés, le timbre *Diffusion Restreinte* doit être apposé au milieu de la page de garde et de la couverture.

Sur les supports numériques *Diffusion Restreinte*, la mention de protection est adaptée au type de support, définitive et toujours visible. Lorsque ce n'est pas possible, un suivi de ces supports est recommandé afin de les répertorier.

4. Conservation, destruction et impression/reproduction

Les documents et supports *Diffusion Restreinte* sont enregistrés au départ et à l'arrivée selon les règles appliquées à tous documents administratifs non classifiés.

Ils doivent être conservés dans des meubles offrant des garanties de sécurité suffisantes (cf. fiche introductive du titre 5).

Leur destruction irréversible a lieu sous la responsabilité des détenteurs, sans mention particulière sur les documents d'enregistrement du courrier, ni procès-verbal²¹⁷.

Leur impression/reproduction doit rester limitée aux seuls besoins du service.

²¹⁶ En cas de difficultés, les services peuvent se rapprocher de la direction des affaires juridiques (DAJ/D2P/DPSP).

²¹⁷ Cf. les dispositions prévues par l'instruction n° 101/DEF/SGA/DMPA/DPC du 29 juillet 2011 relative à la politique et à l'organisation générale de l'archivage du ministère de la défense et des anciens combattants.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.2****5. Expédition et circulation**

La transmission des documents *Diffusion Restreinte* peut être effectuée :

- à l'intérieur d'un local, d'une enceinte ou d'un bâtiment relevant des autorités habilitées à décider de l'emploi du *Diffusion Restreinte*, sans précaution particulière si le convoyeur est une personne autorisée à en connaître ou sous pli fermé dans le cas contraire, par toute personne du ministère de la défense ou par toute personne morale autorisée par le ministère de la défense ;
- vers l'extérieur ou par un tiers :
 - o la transmission s'effectue sous double enveloppe, l'enveloppe intérieure portant la mention *Diffusion Restreinte* et les références du document, l'enveloppe extérieure ne comportant que les indications nécessaires à la transmission,
 - o l'envoi est acheminé en recommandé²¹⁸ avec accusé de réception par voie postale en France métropolitaine, vers les départements et collectivités d'outre-mer (DROM, COM) et vers l'étranger.

Lorsqu'ils sont destinés à une mission diplomatique ou consulaire (et par extension à une mission de défense à l'étranger), les plis doivent porter la mention « recommandé-valise » et sont transmis au SCA/Section valise diplomatique défense qui les achemine par la voie de la valise non accompagnée. La transmission par moyen électronique garantit la protection des informations. Les règles suivantes sont applicables :

- sur un réseau de transmission homologué *Diffusion Restreinte* ou plus, la transmission peut se faire en clair, le *Diffusion Restreinte* doit être cependant chiffré, en fonction du besoin d'en connaître et des accès au réseau ;
- dans les autres cas, les informations sont chiffrées à l'aide d'un dispositif ayant fait l'objet d'une qualification ou d'un agrément de l'ANSSI²¹⁹.

²¹⁸ Recommandé niveau R1.

²¹⁹ Par exemple, outil ACID pour le ministère de la défense.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.3****MENTION COMPLÉMENTAIRE DE PROTECTION *SPECIAL FRANCE*****Références :**

- Code de la défense – article R.2311-4
- IGI 1300 – 1.2.2.1, 2.2.3.2, 6.6.3.1, 7.1.1.3.a, annexes 36 et 37

Points clés

- La mention *Spécial France* n'est pas une mention de classification.
- Elle est apposée sur les documents nationaux, en complément d'autres timbres.
- Il est interdit aux ressortissants étrangers, civils et militaires²²⁰ même habilités, de prendre connaissance, en aucune circonstance, des documents portant la mention *Spécial France*.
- Une personne ne respectant pas les règles de discrétion pour cette mention de protection peut faire l'objet d'une sanction administrative, voire pénale.

1. Champ d'application

La mention *Spécial France* n'intéresse que les documents d'ordre strictement national traitant de sujets que l'autorité estime ne pouvoir être communiqués qu'aux nationaux. Elle est employée pour les informations et supports classifiés ou portant la mention *Diffusion Restreinte* que l'autorité émettrice estime devoir n'être divulgués qu'aux seuls ressortissants français.

Elle peut être apposée sur des informations et supports classifiés mais aussi sur des documents faisant l'objet de la mention de protection *Diffusion Restreinte*. Dans l'objectif d'une passation de marché public, la mention *Spécial France* doit être étudiée et portée après l'acceptation des parties, de l'entité contractante et de l'occupant bénéficiaire de la prestation, en amont de sa signature. Cette mention n'est pas une mention de classification et peut ne concerner que certaines parties d'un document.

Lorsque des informations marquées *Spécial France* sont classifiées, elles doivent, outre satisfaire aux mesures de sécurité appropriées à leur mention, n'être transmises qu'à des personnes physiques et morales françaises dûment habilitées et ayant le besoin d'en connaître. Ce principe implique un cloisonnement des informations *Spécial France* qui peut être assuré par des mesures techniques ou organisationnelles afin d'en limiter l'accès aux seules personnes de nationalité française. De la même manière, ce principe impose des règles de conservation strictes pour n'en permettre l'accès qu'aux personnes dûment autorisées.

2. Marquage

Le timbre est de couleur bleue. Il est apposé en haut de page, immédiatement à droite ou au-dessous du timbre de classification (ou de la mention de protection *Diffusion Restreinte*).

²²⁰ Y compris les officiers de liaison ou officiers d'échange insérés dans une unité française.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.3****3. Mesures de sécurité**

Les mesures de sécurité à appliquer sont déterminées par la mention de protection *Diffusion Restreinte* ou de classification du document ou du support. Leur acheminement se fait par des voies nationales. Elles ne figurent en aucun cas sur des inventaires ou répertoires prescrits par les règlements de sécurité relatifs aux accords internationaux.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.4****MENTION COMPLÉMENTAIRE DE PROTECTION COMMUNICABLE
À [SERVICES, ÉTATS, ORGANISATIONS INTERNATIONALES,
INSTITUTIONS, ORGANES OU ORGANISMES DE L'UE]****Référence :**

- Code de la défense – article R.2311-4
- IGI 1300 – 7.1.1.3.b

Points clés

- La mention *Communicable à* n'est pas une mention de classification.
- Elle est apposée sur les documents nationaux, en complément d'autres mentions.
- Le personnel ne respectant pas les règles de discrétion pour cette mention de protection peut faire l'objet d'une sanction administrative, voire pénale.

1. Champ d'application

La mention *Communicable à* intéresse les documents traitant de sujets que l'on estime ne pouvoir communiquer qu'à certains services, États, organisations internationales, institutions, organes ou organismes de l'Union européenne. Elle a pour effet de circonscrire expressément le périmètre de diffusion de ces informations et supports ainsi que d'attirer l'attention sur le strict besoin d'en connaître. Elle est apposée par l'auteur du document sous la responsabilité de l'autorité émettrice. Elle est employée pour les informations et supports classifiés ou portant la mention *Diffusion Restreinte* et conformément aux dispositions nationales ou internationales en vigueur.

Elle peut être apposée sur des documents classifiés ou faisant l'objet d'une confidentialité spécifique. La mention *Communicable à* n'est pas une mention de classification. Elle concerne la totalité d'un document.

Lorsque des informations marquées *Communicable à* sont classifiées, elles doivent, outre satisfaire aux mesures de sécurité appropriées à leur mention de protection, n'être transmises qu'à des personnes physiques et morales dûment habilitées et ayant le besoin d'en connaître. Ce principe implique un cloisonnement des informations, qui peut être assuré par des mesures techniques ou organisationnelles. De la même manière, ce principe impose des règles de conservation strictes pour n'en permettre l'accès qu'aux personnes dûment autorisées.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.4****2. Marquage²²¹**

Le timbre est de couleur rouge. Il est apposé en haut de page immédiatement à droite ou au-dessous du timbre de classification, s'il existe. Il précise explicitement les services, États, organisations internationales, institutions, organes ou organismes auxquels le document est communicable.

COMMUNICABLE À

3. Mesures de sécurité

Les mesures de sécurité à appliquer sont déterminées par la mention de protection ou de classification du document ou du support et conformément aux dispositions spécifiques nationales et internationales en vigueur. Leur acheminement est réalisé de façon à garantir le respect du périmètre de diffusion délimité.

²²¹ Sauf dispositions contraires prévues par l'accord intergouvernemental en vigueur.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5****MENTIONS DE CONFIDENTIALITÉ SPÉCIFIQUES****Références :**

- Code de la défense – articles L.4137-1 et R.2311-4
- Code de la santé publique – article R.4127-4
- Code des relations entre le public et l’administration – articles L.311-1 et suivants
- Instruction ministérielle n° 26209/ARM/SGA/DAJ du 16 août 2017 relative à la communication par les services du ministère des armées des documents administratifs aux citoyens

Points clés

- Les mentions de confidentialité spécifiques n’ont pas pour objet de protéger des informations qui relèvent du secret de la défense nationale.
- Le personnel ne respectant pas les règles de discrétion pour ces mentions de confidentialité peut faire l’objet d’une sanction disciplinaire, professionnelle, voire pénale²²².
- Les règles de protection *Diffusion Restreinte* et *Spécial France* sont également applicables aux documents portant une mention de confidentialité spécifique.
- Les mentions *Confidentiel Industrie* ou *Confidentiel Technologie* peuvent être utilisées par le personnel du ministère de la défense et les personnes morales si elles le jugent nécessaire, dans le cadre, notamment, des négociations menées avec l’État qui n’ont pas nécessairement vocation à constituer des informations stratégiques relevant du secret des affaires.
- Les mentions de confidentialité spécifiques ne font pas obstacle à elles seules à la communication d’un document administratif à une personne qui en ferait la demande en application du titre III du code des relations entre le public et l’administration.

1. Généralités

Les mentions de confidentialité spécifiques sont distinctes des mentions liées au secret de la défense nationale. Elles contribuent au respect des autres secrets protégés par la loi ainsi qu’à la protection des informations sensibles en apportant le marquage nécessaire pour attirer l’attention du détenteur et des personnes ayant accès au document.

Leur objectif principal est de sensibiliser l’utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par ces mentions.

La divulgation non autorisée de ces informations peut être de nature à compromettre gravement les intérêts de l’organisme concerné en portant atteinte à son potentiel scientifique et technique, à ses positions stratégiques, à ses intérêts commerciaux ou

²²² Abus de confiance, violation du secret professionnel ou de non-respect des règles relatives au traitement des données à caractère personnel.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

financiers, son personnel, l'organisation d'examens ou de concours, ou à sa capacité concurrentielle. Elles permettent d'indiquer le domaine couvert par la protection : *Confidentiel Personnel*, *Confidentiel Protection Personnel*, *Confidentiel Médical*, *Confidentiel Technologie*, *Confidentiel Industrie*, *Confidentiel Commercial*, *Confidentiel Concours*.

L'obligation de confidentialité et de discrétion qu'imposent les mentions de confidentialité spécifiques n'est pas soumise au code pénal (à l'exception du secret médical et en cas de violation du secret professionnel). La violation d'une mention spécifique de protection n'est donc pas assortie de sanctions pénales et ne constitue pas une compromission. Les sanctions sont alors de deux ordres :

- disciplinaire (avertissement, mise à pied, mutation ou licenciement, consigne, réprimande, blâme, arrêt, etc.) ;
- professionnelle (retrait notamment partiel ou total, temporaire ou définitif d'une qualification professionnelle, prononcée par décret en Conseil d'État pour les militaires).

L'attribution de ces mentions de confidentialité spécifiques relève des autorités définies au point 2 ci-dessous, qui définissent le champ des informations couvertes par chacune de ces mentions de confidentialité et les personnes ayant besoin d'en connaître, ainsi que les modalités spécifiques de protection et d'utilisation. Elles fixent ces règles dans une note suivant les principes fixés ci-après.

L'employeur doit réaliser une information particulière des personnes liées à son organisme et ayant besoin d'en connaître. Il doit veiller à la signature d'une attestation de responsabilité par les personnes ayant reçu cette information particulière. Elle est conservée par l'officier de sécurité. Le contrat de travail ou de stage comprend une clause de confidentialité pour les personnes ayant accès à ces informations.

Les supports de l'information confidentielle portent le marquage de la mention de confidentialité correspondante. Hormis le timbre portant cette mention de confidentialité, toutes les règles définies pour les mentions *Diffusion Restreinte* et *Spécial France* sont applicables à ces mentions de confidentialité. **Le timbre doit être de couleur rouge et n'être apposé sur les documents papier qu'en haut de la page.**

2. Nature des différentes mentions de confidentialités spécifiques et détermination des autorités habilitées à décider de l'emploi de ces mentions**a. *Confidentiel Médical***

Pour les informations relevant du secret médical concernant une personne, la décision relève du directeur du service de santé des armées. Le secret médical est défini par l'article R.4127-4 du code de la santé publique comme étant le secret professionnel institué dans l'intérêt des patients et qui s'impose à tout médecin. Le secret médical entre dans le cadre de l'article 226-13 du code pénal, qui définit le secret professionnel (cf. fiche 3.10).

Besoin d'en connaître : le personnel médical, paramédical et médico-administratif du ministère de la défense est assujéti aux obligations du secret professionnel médical, dans les limites de leurs responsabilités ayant trait à la prise en charge du patient pour

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

lequel ces informations sont dressées. Les patients ont la possibilité de consulter les dossiers les concernant.

b. *Confidentiel Personnel*

La mention *Confidentiel Personnel* a vocation à protéger les informations relatives à la vie privée ou professionnelle du personnel militaire et civil du ministère de la défense (notations, travaux d'avancement, déroulement de carrière, enquêtes sociales notamment). Cette mention peut être complétée en précisant la catégorie de personnel concernée, par exemple : *confidentiel personnel sous-officier*, *confidentiel officiers généraux*. La décision relève des autorités responsables de la gestion du personnel au sein des différents états-majors, directions et services.

Besoin d'en connaître : le service enquêteur, les autorités hiérarchiques de la personne concernée, le personnel chargé de l'administration des ressources humaines, les services contentieux et les intéressés dans la limite autorisée par les procédures de gestion.

c. *Confidentiel Protection Personnel*

La mention *Confidentiel Protection Personnel* a vocation à protéger les informations qui, dans le cadre des procédures d'instruction des dossiers de contrôle de sécurité, ne sont pas couvertes par le secret de la défense nationale. La décision relève du directeur du service enquêteur.

Besoin d'en connaître : le personnel du service enquêteur, les autorités compétentes pour décider des habilitations ainsi que les officiers de sécurité, les directions du personnel et organismes de gestion pour ce qui concerne les décisions.

d. *Confidentiel Concours*

L'inscription de la mention est de la responsabilité des organisateurs d'un concours, examen, épreuve de sélection au sein du ministère.

Besoin d'en connaître : les autorités hiérarchiques en charge de l'organisation, le personnel chargé de préparer les sujets ou de corriger les copies, le personnel chargé de surveiller le bon déroulement des épreuves. Les convoyeurs en charge du transport des sujets ou des copies ne sont pas autorisés à en prendre connaissance.

e. *Confidentiel Industrie*

La mention *Confidentiel Industrie* a vocation à protéger les informations dont la divulgation peut porter préjudice à des établissements publics ou des personnes morales de droit privé lorsqu'elles ressortent du secret en matière industrielle hors contrat impliquant l'accès ou la détention d'informations et supports classifiés. Cette mention peut couvrir :

- l'acquisition de certains matériels ;
- la politique industrielle ;
- les rapports des commissaires du gouvernement ;
- les données industrielles des directions et services techniques de la défense ;

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

- les échanges entre le service enquêteur et les autorités d'habilitation ou contractantes dans le cadre des procédures d'habilitation des établissements industriels.

Cette mention peut être complétée par le nom de la société ou de l'organisme d'État lorsqu'il s'agit de protection des droits de propriété industrielle ou intellectuelle.

f. *Confidentiel Technologie*

La mention *Confidentiel Technologie* a vocation à protéger les informations dont la divulgation peut porter atteinte au secret en matière de recherche ou de technologie, dans la mesure où elles ne relèvent pas du secret de défense. Cette mention peut être complétée par le nom de la société ou de l'organisme d'État lorsqu'il convient de sauvegarder l'identité de ces derniers ou leurs droits sur les résultats des recherches, en vue de leur exploitation ultérieure.

g. *Confidentiel Commercial*

La mention *Confidentiel Commercial* a vocation à protéger les informations relatives à des négociations commerciales menées pour le compte d'établissements industriels de la défense ou effectuées dans le cadre d'exportation de matériels d'armement dont il convient de préserver la confidentialité.

Besoin d'en connaître (*Confidentiel Industrie, Confidentiel Technologie et Confidentiel Commercial*) : dans la limite de leurs responsabilités et de leurs attributions dans les domaines concernés notamment en matière de recherches, de programmes ou de passation des contrats :

- pour le personnel de la DGA, du SGA, de la DRSD, des états-majors, directions et services directement intéressés ;
- pour le personnel des personnes morales ou de laboratoires du secteur national ou privé dans le cadre des contrats passés avec des organismes relevant du ministère.

L'attribution des mentions *Confidentiel Industrie, Confidentiel Technologie et Confidentiel Commercial* relève du DGA, du SGA, du chef du Contrôle Général des Armées, des autorités responsables de la gestion des matériels dans les états-majors et grandes directions ainsi que de la DRSD dans le cadre de la protection du patrimoine de l'industrie de défense.

3. Élaboration et marquage

L'élaboration des documents de confidentialité spécifique doit être effectuée dans les locaux des responsables d'organisme directement concernés et sous leur responsabilité, par des personnes présentant les garanties de discrétion de par leur statut ou leur lien contractuel avec ces autorités.

Les documents de confidentialité spécifique doivent porter les marquages suivants :

- sur la première page, les références : organisme émetteur, date d'émission, numéro d'enregistrement ;
- sur chaque page, le timbre adapté avec encre rouge, apposé au milieu du haut ;
- pour les documents reliés, le timbre adapté est placé au milieu du bas de la page de garde de la couverture.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5****4. Circulation et expédition**

À l'intérieur d'un service, la transmission de ces documents s'effectue sans précaution particulière si le convoyeur est une personne autorisée à en connaître ou sous pli fermé dans le cas contraire.

Vers l'extérieur ou par un tiers, la transmission des documents doit respecter les règles suivantes :

- sous double enveloppe, soit par voie postale, soit par porteur autorisé (cf. fiche 7.8) ;
- l'enveloppe intérieure porte la mention de « confidentialité spécifique » et les références du document ;
- l'enveloppe extérieure ne porte que les indications nécessaires à sa transmission.

L'envoi doit être acheminé en recommandé avec accusé de réception :

- en France métropolitaine et vers les DROM-COM par voie postale ;
- vers l'étranger par voie postale et par valise diplomatique.

L'utilisation de bordereaux récapitulatifs de pièces est recommandée ; il appartient à l'expéditeur d'en apprécier l'opportunité en fonction de la nature de l'envoi et des moyens d'acheminement utilisés.

La transmission des informations de confidentialité spécifique par moyen électronique doit appliquer la même procédure que pour le *Diffusion Restreinte Spécial France* (cf. fiche 7.2). Celle-ci fait l'objet de mesures particulières portant sur l'identification des correspondants, l'approbation des circuits ou la protection des données par moyen de chiffrement qualifié au niveau adéquat.

5. Conservation, impression/reproduction et destruction

Les documents de confidentialité spécifique sont enregistrés au départ et à l'arrivée.

Ils doivent être conservés dans des locaux ou dans des meubles offrant des garanties de sécurité suffisantes (*a minima* fermés à clés) pour éviter leur divulgation aux personnes non autorisées.

Leur impression/reproduction est laissée à l'initiative du destinataire et sous sa responsabilité, sauf mention contraire de l'autorité d'origine.

Le destinataire est responsable de leur destruction par des moyens ou procédés offrant toute garantie de sécurité.

Les livrets médicaux détenus par le service de santé des armées ne font pas l'objet d'une mention de confidentialité spécifique mais sont couverts par le secret médical. Ils sont conservés de manière à empêcher tout accès à des personnes n'ayant pas le besoin d'en connaître. Des dispositions de protection mécanique sont nécessaires pour assurer la sécurité des locaux conservant ces livrets. Ils sont complétés par des dispositifs de protection électronique, si nécessaire.

6. Communication des informations de confidentialité spécifique

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.5**

Ces documents sont par principe communicables qu'aux personnes ayant le besoin d'en connaître.

Toutefois, les documents à caractère nominatif sont communicables à la personne intéressée, au sens des dispositions de l'article L.311-6 du code des relations entre le public et l'administration (CRPA).

Enfin, ces mentions ne font pas obstacle en elles-mêmes à la communication d'un document administratif à toute personne qui en ferait la demande en application de l'article L.311-1 du code des relations entre le public et l'administration, sous réserve des secrets protégés par les articles L.311-5 (par exemple la conduite de la politique extérieure de la France, la sûreté de l'État, la sécurité publique, la sécurité des personnes ou la sécurité des systèmes d'information des administrations) et L.311-6 du même code (par exemple la protection de la vie privée, le secret médical ou le secret des affaires²²³).

²²³En cas de difficultés, les services peuvent se rapprocher de la direction des affaires juridiques (DAJ/D2P/DPSP).

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.6****CAS PARTICULIER DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TRÈS SECRET CLASSIFICATION SPÉCIALE****Références :**

- Code de la défense – articles R.2311-1 à 2311-5
- IGI 1300 – 1.3.1 et 7.2.1.2

Points clés

- La protection des informations et supports classifiés *Très Secret* classification spéciale est organisée dans le cadre d'une réglementation particulière du Premier ministre, qui complète les dispositions de caractère général de l'IGI 1300 ; elle s'opère dans le cadre d'une chaîne de sécurité distincte de celle des officiers de sécurité.
- L'élaboration, le traitement, le stockage, l'acheminement, la présentation ou la destruction des informations et supports classifiés au niveau *Très Secret* classification spéciale nécessitent une autorisation du SGDSN.

1. Principes

Le *Très Secret* classification spéciale est réservé aux informations et supports classifiés concernant des priorités gouvernementales en matière de défense et de sécurité nationale. Les modalités de protection et de gestion de ces informations et supports classifiés sont déterminées par le Premier ministre.

Aucun service ni organisme ne peut élaborer, traiter, stocker, acheminer, présenter ou détruire des informations ou supports classifiés *Très Secret* classification spéciale sans y avoir été préalablement autorisé par le SGDSN.

Le versement aux archives des informations et supports classifiés *Très Secret* classification spéciale n'est possible qu'après une procédure, obligatoire et préalable, de déclassement ou de déclassification.

2. Une chaîne de protection du secret distincte de la chaîne classique

La protection des informations et supports classifiés faisant l'objet d'une classification spéciale relève d'une chaîne de protection spécifique définie par le Premier ministre.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.7****ENREGISTREMENT ET INVENTAIRE****Référence :**

- IGI 1300 – 7.2.2 et 7.4

Points clés

- Les règles d'enregistrement et d'inventaire des informations et supports classifiés permettent d'assurer leur traçabilité et leur prise en compte par les détenteurs habilités.
- Par principe, les documents assurant la gestion des informations et supports classifiés ne sont pas classifiés sauf s'ils contiennent les objets eux-mêmes classifiés des documents enregistrés.
- Le niveau de classification des systèmes d'enregistrement, comme des inventaires, est équivalent au niveau de classification des documents qu'ils référencent ou inventorient lorsque leur objet est mentionné et qu'il est lui-même classifié²²⁴.
- Il est recommandé de ne pas mentionner l'objet des documents classifiés lors des enregistrements et des inventaires afin de faciliter leur gestion.
- Un inventaire contradictoire est effectué à chaque changement de détenteur.
- Un inventaire des informations et supports classifiés « papier » et des supports numériques est effectué chaque année²²⁵. Celui des informations classifiées dématérialisées n'est pas obligatoire.
- Une période ouvrée doit être banalisée et spécifiquement dédiée à l'inventaire annuel ou lors du départ du détenteur.

1. Enregistrement

Le but de l'enregistrement est d'établir sans ambiguïté l'attribution d'informations et supports classifiés à un détenteur, c'est-à-dire une personne physique clairement identifiée. Tout information et support classifié est enregistré, dans l'ordre chronologique, dans un système d'enregistrement spécifique, manuel ou informatisé (le système ou fichier doit alors être régulièrement sauvegardé notamment sur un support externe)²²⁶, dont l'accès est restreint aux personnes ayant le besoin d'en connaître.

²²⁴ Par principe, l'objet d'un document est classifié au même niveau que le document lui-même, sauf si son auteur en décide autrement et le précise.

²²⁵ Les services d'archives définitives et intermédiaires du ministère répondent à des dispositions qui leurs sont propres.

²²⁶ Un support amovible est enregistré comme un seul document même s'il contient plusieurs fichiers et ceux-ci sont inscrits dans le document d'enregistrement. La traçabilité intrinsèque du support dématérialisé permet de connaître les fichiers qu'il contient ou qu'il a contenus.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.7**

Si l'objet des documents est classifié²²⁷ et est mentionné dans le système d'enregistrement (manuel ou informatisé), celui-ci est classifié au même niveau que les documents qu'il référence. Dans ce cas, les personnes qui le manipulent doivent être habilitées au niveau requis et le système numérique qui l'héberge, le cas échéant, homologué à ce niveau. Si l'auteur d'un document a précisé que son objet n'était pas classifié, il peut être enregistré dans un système non classifié²²⁸.

Pour les informations classifiées dématérialisées, le traçage est assuré automatiquement par le système numérique, conformément aux obligations de traçabilité qui lui sont imposées par l'IGI 1300. La matérialisation d'une information classifiée dématérialisée (impression, CD-ROM, etc.) est tracée et enregistrée. De même, les transferts d'un système numérique classifié à un autre système numérique classifié sont tracés (éventuellement par une passerelle).

Pour les informations et supports classifiés matériels (papiers et supports numériques), le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par l'émetteur sont inscrits dans le système d'enregistrement. Ce numéro apparaît sur chaque information et support classifié. Le détenteur assume alors la responsabilité de la protection du support. Cet enregistrement est la seule référence de cette attribution de responsabilité. Pour un support numérique, dans la mesure du possible, le numéro d'enregistrement est assorti d'une fiche où sont inscrites les références des informations contenues.

La position des supports classifiés est suivie sans discontinuité, notamment dans le système d'enregistrement des supports classifiés (cf. annexe 15 - modèle de fiche de position).

Enfin, pour chaque support classifié, il est précisé dans le système d'enregistrement l'échéance de classification ou, à défaut, la date ou le délai de réévaluation impérative du niveau de classification fixé par l'auteur de l'information.

Un modèle des renseignements qui doivent se trouver dans le système d'enregistrement (papier ou dématérialisé) est donné en annexe 16.

a. Au niveau Secret

Un système d'enregistrement, mis en place par le responsable de l'organisme avec l'appui de l'officier de sécurité, est tenu par le service en charge de la gestion des informations et supports classifiés de ce niveau (bureau de protection du secret, le cas échéant). Il peut être relié à une base de gestion du courrier sous réserve que l'accès à la base soit restreint aux seules personnes autorisées et habilitées, si le système contient les objets des documents et que ceux-ci sont classifiés et qu'elle permette de tracer les détenteurs jusqu'au document final. Dans ce cas, la base de gestion du

²²⁷ Il est primordial d'adopter le principe de marquage de l'objet (cf. §7.1.4. a) pour identifier rapidement le niveau de celui-ci. En l'absence de marquage particulier, l'objet est par défaut du même niveau que le document lui-même.

²²⁸ À l'exception d'informations et supports classifiés de niveau *Très Secret*, dont l'enregistrement doit s'effectuer sur un système classifié.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.7

courrier doit être hébergée sur un système numérique homologué au niveau de classification requis.

b. Au niveau *Très Secret*

Le bureau de protection du secret assure l'enregistrement des informations et supports classifiés sur un système d'enregistrement. Par principe, ce système est classifié au niveau *Très Secret*. Sa classification peut toutefois être limitée au niveau *Secret* si les objets des informations et supports enregistrés n'y sont pas mentionnés ou si ces derniers ont tous été expressément déclassifiés ou déclassés par leur auteur. Chaque support d'informations et supports classifiés à ce niveau fait l'objet d'une double numérotation présentée sous la forme d'une fraction comportant le numéro d'enregistrement de l'auteur sur le numéro d'enregistrement du bureau de protection du secret chargé de leur traitement

2. L'inventaire

L'inventaire consiste à vérifier la concordance entre le stock physique effectif des informations et supports classifiés et ceux listés dans les registres. Il est classifié au même niveau que les documents qu'il inventorie si l'objet des documents y figure et qu'il est lui-même classifié. Les services d'archives répondent à des dispositions d'inventaire qui leurs sont propres.

Au moment de l'inventaire, chaque organisme détenteur vérifie, (cf. fiche 7.12) si les supports qu'il détient ont fait l'objet d'une déclassification. Chaque autorité émettrice procède à l'examen de classification des documents qu'elle a émis et, dans le cas contraire, chaque fois que possible, à leur déclassification, ou, à tout le moins, à leur déclasserement.

Un document de travail (par exemple : brouillon, courriel, etc.) est identifié, protégé et suivi mais ne nécessite pas d'être inventorié (cf. fiche 7.1).

L'inventaire des informations classifiées dématérialisées au sein d'un système numérique n'est pas nécessaire, leur suivi étant assuré par la traçabilité interne du système numérique renforcée par les exigences organisationnelles et logiques prévues par la PSSI ministérielle (pour le département ministériel) ou par la présente instruction pour les personnes morales contractantes.

L'inventaire est réalisé lors d'une mutation ou annuellement :

- lors du changement de titulaire d'un emploi figurant au catalogue des emplois, il est procédé à un inventaire détaillé contradictoire entre les titulaires montant et descendant et signé des deux personnes. Cet inventaire est enregistré et conservé au niveau de l'organisme et permet de connaître le détenteur actuel de l'information et support classifiés (cf. annexe 17) ;
- un inventaire des informations et supports classifiés matériels (supports et documents papier) est réalisé chaque année et arrêté au 31 décembre. Les dates d'expiration de validité sont vérifiées aux fins de déclasserement ou de déclassification : la réévaluation du niveau de protection des informations et supports classifiés est réalisée et, le cas échéant, leur destruction ou leur versement aux archives est étudié.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.7****a. Au niveau Secret**

Un inventaire annuel est effectué sous la responsabilité de chaque détenteur qui doit être en mesure de le présenter aux personnes en charge de la gestion des informations et supports classifiés et à l'officier de sécurité.

b. Au niveau Très Secret

L'inventaire annuel est effectué par les détenteurs sous la supervision du bureau de protection du secret. Le procès-verbal d'inventaire annuel mentionne les références et l'identification de chaque support classifié *Très Secret* et est accompagné, le cas échéant, de l'une ou l'autre des pièces administratives suivantes :

- un bordereau de prise en compte ;
- un procès-verbal de destruction (fiche 7.13) ;
- une fiche de suivi du support (IGI 1300 – 7.3.2.1.a et fiche 7.8) ;
- un procès-verbal de versement à un dépôt d'archives.

Banalisation d'une période dédiée à l'inventaire :

Chaque responsable d'organisme arrête une période ouvrée dédiée à l'inventaire, au cours de laquelle les détenteurs sont déchargés de leurs missions habituelles.

De même, le responsable d'organisme accorde à chaque personne détenant des informations et supports classifiés quittant ses fonctions une période lui permettant de procéder à son inventaire.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8****DIFFUSION ET TRANSPORT DES INFORMATIONS ET SUPPORTS
CLASSIFIÉS****Références :**

- IGI 1300 – 7.3. et annexes 41 à 44
- Instruction n° 132/ARM/SGA/SPAC du 14/12/2017 relative au traitement des valises diplomatiques vers ou depuis l'étranger pour le compte du ministre des armées
- Instruction n° 133/ARM/SGA/SPAC du 14/12/2017 relative à la transmission des courriers classifiés en partance ou en provenance des départements ou régions français d'outre-mer et collectivités d'outre-mer

Points clés

- La transmission physique d'informations et supports classifiés répond à des modalités précises, différenciées suivant le niveau de classification et le lieu de destination.
- La transmission dématérialisée d'informations classifiées *via* un système numérique homologué doit être privilégiée à l'envoi de supports physiques (papier, CD-ROM, etc.).
- Quel que soit le mode de transport, la traçabilité des informations et supports classifiés est toujours assurée.

1. Cas général de transmission physique d'informations et supports classifiés

Lorsqu'une information classifiée ne peut être diffusée *via* un système informatique homologué, une transmission physique n'est possible que selon les modalités décrites dans les tableaux présentés dans cette fiche. Lorsque l'envoi au moyen d'un système numérique homologué au bon niveau est possible, son utilisation est autorisée et l'envoi par voie postale est alors interdit.

- Si la diffusion de l'information se fait lors d'une réunion, les prescriptions de la fiche 5.4 de la présente instruction doivent être appliquées.
- **L'expédition par voie postale d'informations et supports classifiés de niveau *Très Secret* est interdite.**
- **Pour l'expédition par voie postale d'informations et supports classifiés de niveau *Secret* :**
 - L'emploi du recommandé de niveau R3 avec accusé de réception est privilégié.
 - La preuve de dépôt du recommandé ainsi que la preuve de distribution du recommandé sont archivées par le bureau de protection du secret ou le bureau courrier en charge des informations et supports classifiés.
 - Si le bureau de protection du secret ou le bureau courrier en charge des informations et supports classifiés passe par un vaguemestre pour l'envoi postal, une prise en charge de l'enveloppe est assurée (notion de traçabilité).

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

- Si un bureau courrier ou un secrétariat reçoit un recommandé contenant des informations et supports classifiés, il doit pouvoir le stocker provisoirement (de plusieurs heures à plusieurs jours) dans un meuble et un local adaptés (cf. fiche introductive du titre 5) avant de pouvoir le remettre au destinataire final.
- Le transport doit impérativement être confié à un opérateur postal autorisé conformément aux dispositions du code des postes et des communications électroniques²²⁹.
- **Les supports marqués *Spécial France* ne peuvent sortir des frontières du territoire que par la valise diplomatique (VD).** Une dérogation validée par l'officier de sécurité de niveau 1 est possible par le biais d'un certificat de courrier approuvé par le SGDSN. Les expéditions vers l'outre-mer impliquent parfois un transit par des pays étrangers et un incident peut amener un vol direct à faire une escale imprévue dans un pays étranger. Dès lors, les expéditions vers ces destinations doivent bénéficier du même niveau de protection qu'un courrier à destination de l'étranger.
- Les procédures d'expédition permettent de respecter des délais compatibles avec le degré d'urgence, d'assurer le suivi et de garantir l'intégrité physique du support classifié grâce à un conditionnement spécial.
- Avant toute diffusion d'informations et supports classifiés, le service émetteur établit la liste des destinataires en s'assurant qu'ils sont habilités au niveau de classification requis. Si cette liste est sensible, elle n'est pas jointe aux informations et supports classifiés.

a. Émission

Les autorités d'expédition sont :

- au niveau *Secret*, les personnes en charge de la gestion des informations et supports classifiés à ce niveau ;
- au niveau *Très Secret*, le bureau de protection du secret (cf. fiche 2.7).

Pour les documents classifiés, le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par l'émetteur sont précisés dans la liste de diffusion (au niveau *Très Secret*, deux exemplaires au moins, dont un original destiné, à terme, aux archives, cf. fiche 7.11). À l'intérieur d'un site ou d'une même emprise, une fiche de suivi, établie pour chaque support classifié au niveau *Très Secret*, permet d'en contrôler la position et est émargée par chaque personne qualifiée y ayant accès. La fiche de suivi est conservée par le bureau de protection du secret dans les mêmes conditions que pour un support classifié au niveau *Très Secret*.

²²⁹ Autorisation délivrée par l'autorité de régulation des communications électroniques et des postes (ARCEP), articles L.36-5 et suivants et R.1-2-1 et suivants du code des postes et des communications électroniques.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

Après marquage et enregistrement de chaque support, il est procédé aux opérations suivantes :

Conditionnement :

L'envoi de supports classifiés se fait sous double enveloppe présentant des garanties de solidité de nature à assurer au maximum l'intégrité physique des supports :

- l'enveloppe extérieure : renforcée et plastifiée, elle porte l'indication du service expéditeur, l'adresse du destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère classifié du contenu) et la mention du suivi. Elle ne porte en aucun cas la mention du niveau de classification de l'information ou du support qu'elle contient ;
- l'enveloppe intérieure de sécurité : opaque, toilée ou armée, elle interdit l'ouverture ou la refermeture discrète. Elle porte le timbre du niveau de classification ou de protection, la référence des supports transmis, le cachet de l'autorité expéditrice, le nom et la fonction du destinataire ainsi que l'indication de l'entité dans laquelle il est affecté.

Suivi de l'envoi :

L'expéditeur reste responsable des informations et supports classifiés transportés jusqu'à sa prise en compte par le destinataire.

Le bordereau d'envoi, sans timbre de classification ni indication de l'objet des informations envoyées, comporte **trois feuillets détachables si possible de couleurs différentes A, B et B'** (cf. IGI 1300 - annexe 41), signés par le responsable de l'autorité expéditrice ou une personne désignée par lui. Ils sont conservés 5 ans :

- les feuillets A (blanc) et B (vert) sont placés dans l'enveloppe intérieure de sécurité et sont adressés au destinataire qui conserve le premier (A) comme élément de preuve et renvoie le second (B) à titre d'accusé de réception ;
- le feuillet B' (rose) est conservé par l'expéditeur jusqu'à réception du feuillet B qui lui est alors substitué.

La différence de couleur des bordereaux permet une visualisation rapide par l'expéditeur des accusés de réception (volets B) manquants.

En cas de convoyage, l'expéditeur s'assure de la date et de l'heure de livraison. Il en avise aussitôt le service destinataire par courrier électronique. Pour les envois postaux, il indique au service destinataire le bureau de dépôt du courrier et les références du support, à l'exclusion de leur objet et de leur caractère secret. La traçabilité physique ou logique doit être assurée en permanence. En cas de retard anormal, il y a suspicion de compromission. Le bureau de protection du secret ou le service destinataire met alors en œuvre les dispositions à suivre en cas de compromission (cf. titre 8).

Les supports classifiés envoyés à l'étranger ou transitant par des pays étrangers doivent être protégés en permanence pour interdire leur compromission pendant le transport, notamment lors des escales. Si l'information ou le support classifié ne transite pas par

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

valise diplomatique, le porteur doit être muni d'un certificat de courrier (cf. définition en annexe 20).

Les modalités de suivi (bordereaux, etc.), décrites ci-dessus, ne concernent que les supports expédiés par voie physique et non les informations transmises de façon dématérialisée.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE

7.8

Transport de documents ou matériels portant la mention *Diffusion Restreinte* et d'informations et supports classifiés sur le territoire national

	Détenteur	Personne du service de courrier interne	Personne habilitée OU Convoyeur autorisé par le ministère de la défense	Voie postale (opérateur autorisé)	Valise diplomatique Porteur muni d'une lettre de courrier ²⁶⁷
Au sein de l'emprise	DR	X	X	Sans objet	Sans objet
	DRSF	X	X	Sans objet	Sans objet
	S	X	X	Sans objet	Sans objet
	TS	X	X	Sans objet	Sans objet
En métropole	DR	Sans objet	X	X	Sans objet
	DRSF	Sans objet	X	X	Sans objet
	S	Sans objet	X	X	Sans objet
	TS	Sans objet	X	Interdit	Sans objet
	DR	Sans objet	X	X ²³⁰	Sans objet
De et vers l'outre-mer	DRSF	Sans objet	Interdit	Interdit	X
	S	Sans objet	+ certificat de courrier ²⁶⁵	X ^{264 et 232}	(de manière exceptionnelle ²³³)
	S-SF	Sans objet	Interdit	Interdit	X
	TS	Sans objet	+ certificat de courrier ²⁶⁵	Interdit	X
	TS-SF	Sans objet	Interdit	Interdit	X

²³⁰ À la condition impérative de confier le transport à La Poste ou une de ses filiales répondant aux conditions du transport postal en métropole. Il est fait usage du service prioritaire « recommandé ».

²³¹ Sont exclus du domaine d'utilisation du certificat de courrier en raison de ses limites d'emploi les documents, équipements et/ou composants classifiés de l'OTAN ; dans ce cas, le certificat de courrier est remplacé par un ordre de mission de courrier établi selon les dispositions des directives OTAN AC/35-D/2002 (appendice 1 à son annexe) et AC/35-D/2003 (appendice 8).

²³² Le recours à un porteur muni d'un certificat de courrier est néanmoins à privilégier. Celui-ci doit être en mesure d'acheminer le pli dans les deux mois qui suivent.

²³³ Le recours à la valise diplomatique est possible uniquement pour les plis. Il convient en ce cas de contacter la section Valise Diplomatique Défense du ministère de la défense (SGA/GSBBDDIDF/PAVP/BGET/SVDD). En raison de leur volume, les colis et équipements ne peuvent être pris en compte.

TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS TOUT AU LONG DE LEUR CYCLE DE VIE 7.8

Transport de documents ou de matériels portant la mention *Diffusion Restreinte* et d'informations et supports classifiés de et vers l'étranger

	Détenteur	Personnel du ministère de la défense ou de l'organisme détenteur habilité ²³⁴ OU Convoyeur autorisé par le ministère de la défense		Voie postale (opérateur autorisé ²⁶³)	Valise diplomatique Porteur muni d'une lettre de courrier ²⁶⁷
OTAN / UE	DR	X	X	X ²⁶⁸	X
	DRSF	interdit	interdit	interdit	X
	S	+ certificat de courrier ²⁶⁵	+ certificat de courrier ²⁶⁵	X ²³⁵	X
	TS	+ certificat de courrier ²⁶⁵	+ certificat de courrier ²⁶⁵	interdit	X
	S ou TS-SF	interdit	interdit	interdit	X
De et vers l'étranger (avec accord de sécurité)	DR	X	X	X ²⁶⁸	X
	DRSF	interdit	interdit	interdit	X
	S	Si prévu par accord + certificat de courrier	Si prévu par accord + certificat de courrier	Si prévu par accord ²⁰⁹ et ²¹⁴	X
	TS	Si prévu par accord + certificat de courrier	Si prévu par accord + certificat de courrier	interdit	X
	S ou TS-SF	interdit	interdit	interdit	X
De et vers l'étranger (sans accord de sécurité)	DR	interdit	interdit	X ²⁶⁸	X
	DRSF	interdit	interdit	interdit	X
	S	interdit	interdit	interdit	X
	TS	interdit	interdit	interdit	X
	S ou TS-SF	interdit	interdit	interdit	X

²³⁴ Au niveau au moins égal à la classification des informations et supports classifiés transporté.
²³⁵ À la condition impérative de confier le transport à La Poste ou une de ses filiales répondant aux conditions du transport postal en métropole. Il est fait usage du service prioritaire « recommandé international ».

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8****b. Réception**

La réception est assurée au niveau *Secret* par le service en charge de la gestion des informations et supports classifiés ou, à défaut, par le destinataire de l'envoi, ou au niveau *Très Secret*, par le bureau de protection du secret de l'entité destinataire, suivant la procédure suivante :

- l'intégrité de l'emballage est vérifiée afin de déceler une éventuelle compromission ;
- l'enveloppe intérieure ne doit être ouverte que par le bureau de protection du secret (obligatoire pour le TS), ou par le service en charge de la gestion des informations et supports classifiés à ce niveau ou le destinataire du courrier (S) ;
- au niveau *Secret*, le destinataire fait procéder à son enregistrement ou au niveau *Très Secret*, le bureau de protection du secret enregistre les informations et supports classifiés ;
- pour le support physique, le feuillet B du bordereau d'envoi est signé et renvoyé à titre d'accusé de réception. Le bureau de protection du secret transmet l'information classifiée *Très Secret* au destinataire.

Ces règles s'appliquent à la réception, par voie physique, des informations et supports classifiés devant faire l'objet d'un enregistrement (cf. fiche 7.7). Dans le cas d'une information classifiée dématérialisée, la réception est assurée par les obligations de traçabilité des systèmes numériques prévues par la présente instruction.

Dans le cas d'un acheminement à l'étranger, le destinataire appose son visa sur la liste d'inventaire présentée par le porteur.

2. Cas particuliers**a. Transport d'informations classifiées sur un support de stockage numérique**

Les informations classifiées conservées sur un support amovible sont, lorsqu'elles sont transportées en dehors d'une zone protégée, acheminées conformément aux règles décrites ci-dessus.

L'utilisation d'un produit ou d'un mécanisme de chiffrement agréé par l'ANSSI, dans le respect des instructions d'emploi associées à cet agrément, permet, conformément aux directives de l'agrément, de déroger aux dispositions du paragraphe relatif au transport de supports classifiés.

b. Matériels classifiés

La circulation et le transport des matériels classifiés nécessitent des mesures particulières de sécurité : protection contre les vues (dans la mesure du possible) et garde permanente pendant la durée du transport.

Pour le niveau *Secret*, à l'étranger, la surveillance permanente par le porteur est systématiquement recherchée par le dépôt du matériel dans une représentation française (consulat, ambassade, coopération, opération extérieure, etc.). Par mesure de précaution, des solutions physiques (étiquettes ou enveloppes de sécurité, etc.) permettent de détecter une tentative d'accès frauduleux au matériel ou une atteinte à son intégrité.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.8**

Un équipement mobile traitant d'informations classifiées fait l'objet de vérifications régulières de sa configuration physique, en particulier avant qu'il soit reconnecté sur le système numérique homologué de son organisme d'appartenance.

Les itinéraires sont choisis en fonction du degré de sécurité qu'ils présentent. Suivant le type de matériel à protéger et dès lors que le matériel transporté figure sur la liste concernant le nucléaire de défense tenue à jour par le ministère de la défense, il convient de se reporter aux dispositions particulières²³⁶.

Pour les autres matériels classifiés, l'autorité en ayant prescrit le mouvement assume la responsabilité des tâches suivantes :

- conditionnement des matériels ;
- choix de l'itinéraire et des lieux d'étape, en accord avec les autorités civiles ou militaires intéressées ;
- organisation du convoi ou de l'escorte et des dispositions techniques en cas de panne ou d'accident.

Les exigences liées au suivi de l'envoi de supports classifiés (bordereau, etc.) sont applicables aux matériels classifiés.

Le transport des matériels classifiés est effectué, sauf impossibilité absolue ou opération conjointe, par des moyens nationaux. À défaut, ils sont convoyés et toutes les dispositions sont prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport. Le recours par voie contractuelle à un transitaire agréé par les autorités portuaires ou aéroportuaires peut être requis lorsqu'il existe des restrictions d'accès à certaines zones aéroportuaires ou maritimes. Dans ce cas, le matériel est placé sous la responsabilité du transitaire qui en assure le suivi (voire le stockage temporaire) entre le moyen de transport (soute de l'avion ou du navire) et la zone où il sera remis au représentant du ministère. Avant tout transfert de matériel classifié, un certificat de courrier (cf. IGI 1300 - annexes 43 et 44) est établi pour le porteur. Un plan de transport peut être exigé par l'autorité nationale de sécurité ou l'autorité de sécurité déléguée compétente, en fonction du poids ou des dimensions du matériel.

²³⁶ Instruction interministérielle n° 3100/SGDN/ACD/PS/DR du 25 juin 1980 sur la sécurité des transports de certains matériels sensibles effectués sous responsabilité civile et directive interministérielle n° 312/SGDN/ANS/DR du 21 août 1981 sur la sécurité nucléaire dans le domaine de la défense.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.9****IMPRESSION/REPRODUCTION DES INFORMATIONS CLASSIFIÉES****Références :**

- IGI 1300 – 7.2.4 et annexes 39 et 40
- IM n° 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées (PSSI-M)

Points clés

- La reproduction et l'impression d'informations et supports classifiés sont placées sous la responsabilité du détenteur.
- Les informations et supports classifiés reproduits doivent être obligatoirement tracés :
 - la traçabilité des informations et supports classifiés papier est organisée par l'officier de sécurité, via la tenue d'un registre (manuel ou informatisé),
 - la traçabilité des informations et supports classifiés dématérialisés est considérée comme étant automatique sur les systèmes numériques classifiés homologués grâce au niveau élevé d'exigences que doivent remplir ces systèmes numériques en matière de traçabilité et d'imputabilité des actions réalisées.
- Les matériels utilisés pour ces actions doivent répondre à des conditions de protection physique et d'homologation pour les matériels connectés sur des systèmes d'information.

Le détenteur est responsable de la reproduction ou de l'impression des informations et supports classifiés qu'il détient.

Les matériels utilisés pour la reproduction d'informations et supports classifiés (photocopieurs, télécopieurs, systèmes numériques, etc.) sont physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées. Si ces matériels sont connectés à un système numérique, ils sont intégrés dans le périmètre d'homologation de ce système numérique et doivent être homologués au même niveau. Les opérations de maintenance sur ces matériels sont effectuées dans des conditions permettant de garantir la sécurité des informations et supports classifiés qui ont été reproduits, dans le respect des dispositions de la présente instruction. Il en est de même pour leur mise au rebut, qui doit garantir la destruction des mémoires de ces appareils.

Le détenteur veille à limiter la diffusion au strict besoin d'en connaître.

1. Au niveau Secret

La reproduction totale est effectuée par le détenteur, sous sa responsabilité, à condition de conserver sur un système d'enregistrement, détenu par les personnes en charge de la gestion des informations et supports classifiés à ce niveau, la trace du nombre et des destinataires des exemplaires papier reproduits (enregistrement et suivi suivant les règles décrites dans la fiche 7.7). Pour les informations et supports classifiés dématérialisés, cette obligation de conservation est assurée automatiquement grâce aux obligations de traçabilité interne du système numérique.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.9**

La reproduction partielle est possible dans les mêmes conditions que la reproduction totale. Les extraits d'informations et supports classifiés ainsi reproduits sont classifiés au même niveau que le document dont ils sont extraits, sauf si l'autorité émettrice les a expressément classifiés à un niveau inférieur ou ne les a pas classifiés.

2. Au niveau *Très Secret*

La reproduction totale ou partielle des informations et supports classifiés de ce niveau n'est possible qu'avec l'autorisation écrite préalable de l'autorité émettrice.

Le détenteur de l'information papier ou sur support classifié qui souhaite en effectuer une reproduction adresse une demande motivée (cf. IGI 1300 - annexe 39) à cette autorité *via* son bureau de protection du secret (BPS, cf. fiche 2.7), en précisant le nombre d'exemplaires. Si l'autorité émettrice consent à la reproduction (cf. IGI 1300 - annexe 40), elle porte mention de cette reproduction sur l'exemplaire en sa possession. Le bureau de protection du secret du détenteur assure l'enregistrement de l'exemplaire unique ou des exemplaires et les fait prendre en compte par les personnes citées dans la demande.

En cas d'urgence et à titre exceptionnel, le détenteur peut s'affranchir de cette procédure et procéder à la reproduction totale ou partielle de l'information et support classifié à la condition de prendre les dispositions suivantes *via* son bureau de protection du secret :

- limiter au minimum indispensable le nombre de reproductions ;
- procéder au marquage réglementaire en attribuant à chaque exemplaire un numéro individuel composé de deux nombres fractionnaires, en numérateur le numéro d'ordre de la copie dans la série des reproductions et en dénominateur le nombre total de reproductions ;
- porter, sur l'exemplaire reproduit, la destination qui en est faite ou établir une liste séparée des destinataires ;
- rendre compte sans délai à l'autorité émettrice du nombre de reproductions, des numéros de reproduction et de la destination des exemplaires. L'autorité émettrice porte mention de cette reproduction sur l'exemplaire en sa possession.

Pour les informations et supports classifiés dématérialisés, ce suivi est assuré par les obligations de traçabilité du système numérique précisées dans la PSSI (entités ministérielles) ou dans la présente instruction.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.10****STOCKAGE DES INFORMATIONS ET SUPPORTS CLASSIFIÉS****Références :**

- IGI 1300 – 7.2.3, § 5.3.3.1
- IM n° 7326-2/DEF/CAB du 25 juin 2018 relative à la politique de sécurité du système numérique du ministère de la défense (PSSI-M)

Points clés

- La responsabilité de la conservation des informations et supports classifiés incombe à leur détenteur.
- Les informations et supports classifiés physiques sont conservés dans des meubles et locaux adaptés.
- Les informations et supports classifiés dématérialisés sont stockés sur un système numérique classifié homologué au même niveau ou au niveau supérieur.

1. Règles générales relatives au stockage des informations et supports classifiés

Chaque information et support classifié fait l'objet d'un suivi de son élaboration à sa déclassification ou à sa destruction. Le responsable d'organisme met en place des moyens de conservation sécurisés et pérennes. La responsabilité de la conservation des informations et supports classifiés incombe à chaque détenteur, au bureau de protection du secret ou aux personnes en charge de la gestion des informations et supports classifiés.

Le traitement ou la conservation d'informations et supports classifiés *Très Secret* ne peut intervenir dans des locaux, sauf en cas d'impossibilité majeure, qu'après l'avis technique d'aptitude physique (ATAP, cf. fiche 5.7) du service enquêteur sur l'aptitude de ces locaux à conserver des informations et supports classifiés de ce niveau.

Les **informations et supports classifiés physiques** sont conservés, en dehors des périodes d'utilisation, dans des meubles et locaux adaptés.

Les combinaisons²³⁷ des meubles sont changées :

- tous les ans ;
- en cas de mutation d'un utilisateur ;
- en cas d'identification d'un risque ou de suspicion de compromission.

Les mesures sont définies par l'IGI 1300 et précisées dans la présente instruction. Pour garantir le cloisonnement, les informations et supports classifiés émis par les États étrangers ou par des organisations internationales sont conservés de façon séparée des informations nationales (cf. fiche 9.4).

Les **informations et supports classifiés dématérialisés** sont conservés sur un système numérique classifié homologué au même niveau ou au niveau supérieur. Les mesures

²³⁷ Il est recommandé d'utiliser une combinaison complexe : 3 nombres différents dont un seul peut finir par « 5 ou 0 » et pour les combinaisons à compteurs un maximum de 3 compteurs dont la valeur est « 0 » ou « 12 ».

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.10**

sont définies par la PSSI ministérielle ou précisées dans le titre 6 de la présente instruction pour les organismes qui ne sont pas soumis à cette dernière. Les exigences de sécurité relatives à la sécurité du système numérique de l'organisme prévoient des moyens et des procédures de sauvegarde et de conservation sécurisés et pérennes des informations classifiées contenues au sein des systèmes numériques classifiés utilisés. Ces moyens et procédures respectent le besoin d'en connaître.

Les systèmes d'information appelés à traiter des informations classifiées doivent faire l'objet d'une homologation (cf. fiches 6.2 et 6.3).

2. Cas particuliers

- Les **informations et supports classifiés dits hors coffre** : des informations et supports classifiés de grande dimension (prototypes ou objets classifiés, par exemple) ne peuvent pas être conservés dans les meubles prescrits pour leur niveau de classification. Dans ces conditions, les règles particulières à appliquer sont précisées dans la fiche 5.3 de la présente instruction.
- Les **moyens mobiles** (aéronefs, navires, etc.) susceptibles de faire escale ou s'implanter temporairement à l'étranger et dans lesquels des informations et supports classifiés sont conservés doivent se conformer aux principes de la fiche 5.3 de la présente instruction (hors opérations, qui répondent à des procédures particulières).

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.11****VERSEMENT DANS UN SERVICE D'ARCHIVES****Références :**

- Code du patrimoine – articles L.212-2, L.212-3, R.212-10, R.212-11 et R.212-65-1
- Arrêté du 28 décembre 2023 fixant la liste des services d'archives du ministère de la défense
- IGI 1300 – 7.5.4 et annexe 46
- Instruction n° 101/DEF/SGA/DMPA/DPC du 29 juillet 2011 relative à la politique et à l'organisation générale de l'archivage du ministère de la défense et des anciens combattants

Points clés

- Les archives intermédiaires et définitives, dont les informations et supports classifiés (TS classification spéciale exclus), sont versées dans des services d'archives relevant du ministère de la défense.
- L'information ou le support classifié ne peut être isolé du dossier auquel il appartient et doit, par conséquent, être versé dans le même fond d'archives. Les services d'archives définitives (Service historique de la défense pour les archives papier et électronique, l'établissement de communication et de production audiovisuelle de la Défense pour l'audiovisuel) sont sollicités pour connaître les lieux de versement.
- Les informations et supports classifiés émis par les États étrangers ou dans le cadre d'organisations internationales doivent être archivés de façon à les séparer clairement des informations nationales.

Avant leur versement, les informations et supports classifiés sont correctement marqués et répertoriés conformément aux modalités de versement définies par le service d'archives destinataire. En outre, le service auteur des informations et supports classifiés vérifie systématiquement la pertinence de la classification et sa durée de vie et décide, le cas échéant, de les déclassifier, de les déclasser ou éventuellement de les reclasser (cf. fiche 7.12). Le service versant, s'il n'est pas le service auteur, vérifie auprès de ce dernier si l'information ou le support est toujours classifié et s'il n'a pas fait l'objet d'un déclassement ou d'un reclassement. Dans le cas où l'information ou le support a fait l'objet d'une décision de déclassification, de déclassement ou de reclassement, le service versant appose le timbre imposé par cette décision.

À l'occasion du versement, le service d'archives peut, s'il le juge opportun, proposer au service émetteur la déclassification ou le déclassement d'un document. Le service auteur reste compétent, au moment du versement, pour décider du niveau de classification des informations et supports classifiés qu'il a produits.

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

7.11

1. Versement aux archives des documents classifiés

On distingue :

- les **archives courantes**, lorsque les documents sont d'utilisation habituelle pour l'activité des services ;
- les **archives intermédiaires**, lorsque, n'étant plus considérées comme archives courantes, les documents ne peuvent encore en raison de leur intérêt administratif faire l'objet d'un tri ou d'une élimination ;
- les **archives définitives**, lorsque les documents ont subi les tris et destructions nécessaires et sont à conserver sans limitation de durée²³⁸.

Les informations et supports classifiés présentant une utilité administrative ou un intérêt historique ou scientifique sont, à l'issue de leur période d'usage courant, versés dans un service d'archives intermédiaires ou définitives. Les autres documents sont détruits (cf. fiche 7.13) après avoir reçu un visa d'élimination conformément à l'article L.212-2 du code du patrimoine.

Le versement dans un service d'archives s'effectue conformément aux principes énoncés par les textes de référence, en suivant les directives données par l'administration des archives et selon les modalités définies par les textes techniques propres à chaque état-major, direction ou service.

Les informations et supports classifiés ne peuvent pas être séparés du dossier auxquels ils appartiennent et du reste de leur fonds d'archives. Il convient de consulter les services d'archives définitives (SHD pour les archives papier et électronique, ECPAD pour l'audiovisuel) pour connaître les lieux de versement déterminés par l'administration des archives (en fonction du type de fonds, de leur intérêt ou de leur ancienneté).

2. Conservation des archives classifiées

Le niveau de classification maximal des informations et supports classifiés qui peuvent être détenus par les différents services d'archives varie d'un service à l'autre mais aucun n'est en mesure d'abriter les informations et supports classifiés de niveau TS faisant l'objet d'une classification spéciale. Ceux-ci doivent faire l'objet d'une procédure de déclassement ou de déclassification.

- a) Les archives définitives et intermédiaires sont conservées par le SHD et l'ECPAD.
- b) Les informations et supports classifiés peuvent également être conservés dans des services d'archives intermédiaires sous contrôle scientifique et technique de la DMCA /DPC²³⁹.
- c) Certaines informations et supports classifiés peuvent enfin être versés dans un service ne relevant pas du ministère, comme les Archives nationales ou le service d'archives des Affaires étrangères²⁴⁰.

²³⁸ Cf. Instruction en référence.

²³⁹ Les services d'archives intermédiaires sont désignés par arrêté du ministre (en référence).

²⁴⁰ Les services du Président de la République, du Premier ministre et des ministères autres que celui de la défense reçoivent des informations et supports classifiés émis par le ministère dans le cadre de leurs fonctions. Les dossiers dans lesquels ces informations et supports classifiés figurent sont versés par la suite aux Archives nationales ou aux Affaires étrangères.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12****DÉCLASSIFICATION OU DECLASSEMENT D'UNE INFORMATION
CLASSIFIÉE****Références :**

- Code du patrimoine – articles L.213-1 et suivants
- IGI 1300 – 1.2.3 et 7.6
- Instruction n° 2264/ARM/CAB/HFCDS sur la Commission de déclassification des archives et son fonctionnement du 27 avril 2022

Points clés

- La date ou l'événement entraînant la déclassification ou la réévaluation de la classification du document doit être indiqué en couverture du document lors de sa classification.
- L'expiration des délais prévus par l'article L.213-2 du code du patrimoine entraîne la déclassification automatique des documents. À l'inverse, la déclassification d'un document ne suffit pas à le rendre communicable de plein droit. Malgré la déclassification, les délais définis par le code du patrimoine sont susceptibles de s'appliquer.
- Les informations et supports classifiés qui ne comportent pas de mention d'échéance de classification et qui n'ont pas atteint l'échéance de communicabilité prévue par le code du patrimoine sont déclassifiés après décision de déclassification par le service auteur ou son successeur, par le HFCDS ou par le Service historique de la Défense pour les documents qu'il conserve.
- Le ministre a toute latitude pour organiser et déléguer le traitement des procédures de déclassification du ministère.
- Pour les informations et supports classifiés étrangers, seule l'autorité étrangère émettrice peut procéder à une déclassification ou à un déclassement.

1. Définitions

La **déclassification** consiste à ôter à une information ou un support classifié la protection particulière qui lui était conférée au titre du secret de la défense nationale. Par défaut, les informations ou supports déclassifiés du ministère de la défense sont protégés par la mention *Diffusion Restreinte* sauf décision contraire de l'émetteur.

Le **déclassement** est la modification, par abaissement, du niveau de classification d'une information ou d'un support classifié (ne s'applique qu'aux niveaux *Très Secret* et *Très Secret* classification spéciale).

Le **reclassement** consiste à apposer sur un document le niveau de classification supérieur.

2. Échéance de la classification

La déclassification d'informations et supports classifiés portant un marquage de classification français peut intervenir selon les conditions suivantes :

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12****a. Informations et supports classifiés portant un marquage de classification national****- de manière automatique, à l'échéance indiquée sur le document**

Lors de l'élaboration d'informations et supports classifiés, la date précisant sa déclassification ou, exceptionnellement, la date ou le délai au terme duquel le niveau de classification doit être réévalué, est porté sur cette information ou ce support classifié.

Des directives techniques rédigées par les états-majors, directions et services encadrent les modalités de déclassification et précisent, pour chaque grande catégorie de documents, les délais de déclassification recommandés (cf. fiche 7.1).

- de manière automatique, à l'échéance des délais de communicabilité fixés par le code du patrimoine

Tout document classifié est automatiquement déclassifié dès lors qu'il devient communicable de plein droit en application de l'article L.213-2 du code du patrimoine (en général au terme d'un délai de cinquante ans). En cas d'absence de date de déclassification, la date de création du document est prise en référence.

- pour les documents non encore librement communicables, à la suite d'une décision du service auteur (Point 4.)

Cette décision peut, notamment, résulter d'une requête en déclassification judiciaire ou d'une demande d'autorisation de consultation par dérogation (demande d'accès anticipée) de documents d'archives publiques avant expiration des délais de communicabilité fixés par le code du patrimoine.

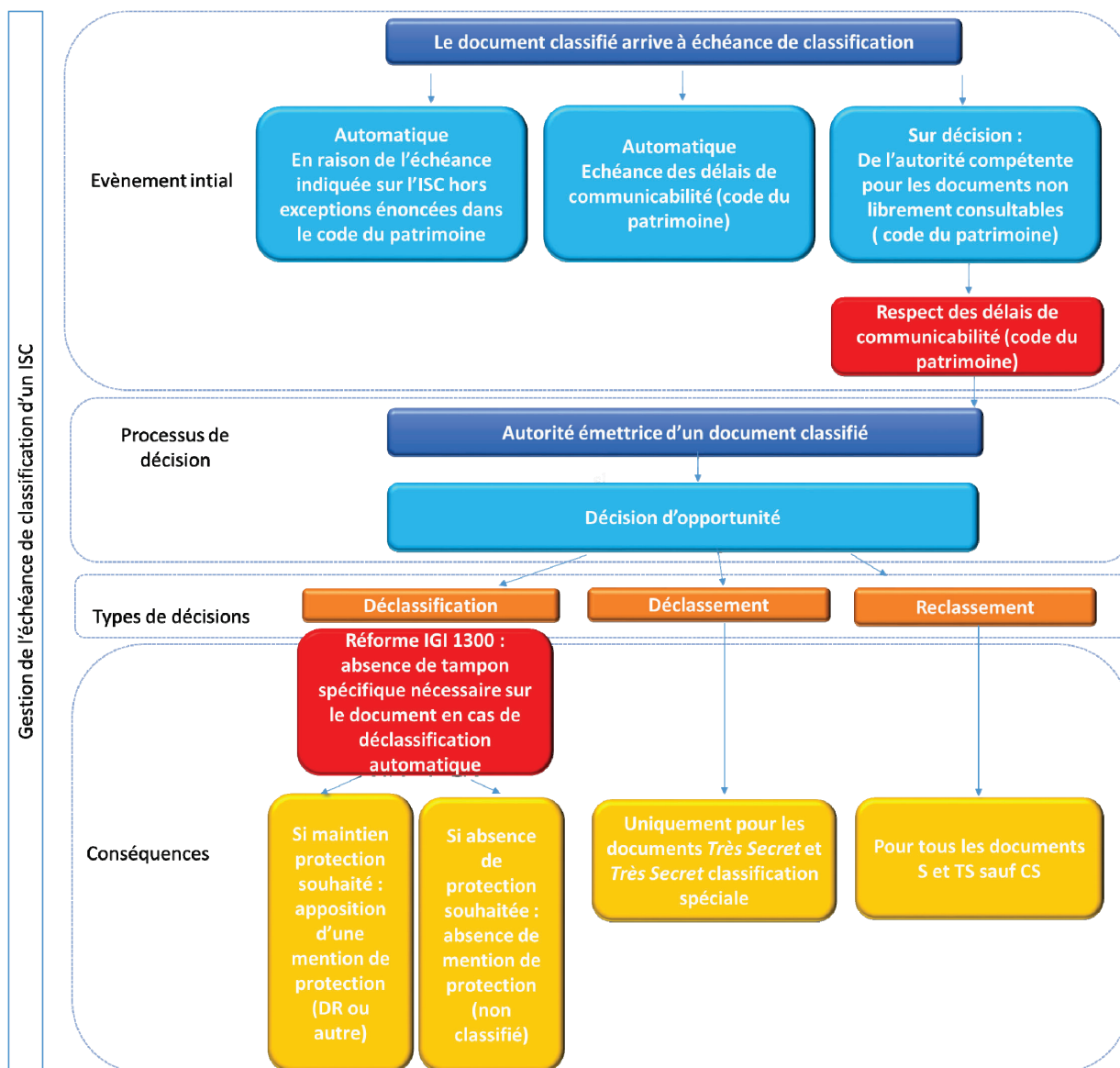
b. Informations et supports classifiés portant un marquage de classification étrangère

Seule l'autorité étrangère émettrice d'informations et supports classifiés portant un marquage de classification étrangère peut procéder à sa déclassification, à son déclasserement ou reclassement.

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

7.12

Schéma de synthèse



**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12****3. La commission de déclassification du ministère de la défense**

Afin de simplifier et d'optimiser l'instruction des demandes de déclassification, de faciliter l'accès aux archives publiques qui peuvent être déclassifiées, tout en protégeant celles qui doivent encore être couvertes par le secret de la défense nationale, et de bâtir en la matière une politique ministérielle cohérente et pertinente, a été créé la commission de déclassification. Cette commission, interne au ministère de la défense, a pour objet d'éclairer et d'accélérer la prise de décision de ses services auteurs en matière de déclassification des documents couverts par le secret de la défense nationale conservés dans les services d'archives définitifs comme intermédiaires.

Pour que la commission de déclassification puisse éclairer la décision portant sur la levée ou non de la protection du secret de la défense nationale concernant un document ou un lot de documents, celui-ci doit :

- avoir été émis par les armées ou au titre du ministère de la défense ;
- avoir été versé et donc être conservé au SHD, à l'ECPAD, dans un service d'archives intermédiaires du ministère de la défense ou dans un service d'archives extérieur au ministère (principalement aux Archives nationales et à la direction des archives du ministère de l'Europe et des Affaires étrangères).

4. Communicabilité des documents

La déclassification d'un support n'entraîne pas pour autant automatiquement la libre communicabilité de ce support ou des informations qu'il contient. Ainsi, l'administration saisie d'une demande de communication d'une information ou d'un support régulièrement déclassifié doit s'assurer qu'aucun autre motif d'incommunicabilité ne trouve à s'appliquer en vertu des articles L.213-2 et suivants du code du patrimoine et de l'article L.311-5 du code des relations entre le public et l'administration.

Il convient, à cet égard, de souligner que les délais d'incommunicabilité mentionnés à l'article L.213-2 sont, pour la plupart d'entre eux, décomptés à partir « *de la date du document ou du document le plus récent inclus dans le dossier* ». Tel est notamment le cas du délai de 50 ans prévu pour les documents dont la communication porte atteinte au secret de la défense nationale. Ces dispositions doivent être interprétées comme prescrivant un décompte à partir de la date du document demandé, quand celui-ci est isolé, et à partir de la date du document le plus récent inclus dans le dossier, dans le cas contraire.

Le « *dossier* », au sens de l'article L.213-2 du code du patrimoine, ne doit pas être assimilé au carton d'archives, en tant que pièce matérielle, au sein duquel se trouve le document dont la communication est sollicitée. Il doit être regardé comme l'ensemble des pièces présentant un lien suffisamment marqué avec le document demandé. Une telle interprétation implique une appréciation, par l'administration, sous le contrôle du juge administratif, du caractère suffisant du lien en question.

Par dérogation aux dispositions de l'article L.213-1 et du I de l'article L.213-2 du code du patrimoine, les informations et supports classifiés dont la divulgation est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12**

localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de niveau analogue sont perpétuellement incommunicables à tout tiers, que ces documents soient classifiés ou non.

En outre, la communication d'un document, bien que déclassifié, ne doit pas porter atteinte à l'un des secrets protégés par les articles L.311-5 (par exemple la conduite de la politique extérieure de la France, la sûreté de l'État, la sécurité publique, la sécurité des personnes ou la sécurité des systèmes d'information des administrations) et L.311-6 du code des relations entre le public et l'administration (par exemple la protection de la vie privée, le secret médical ou le secret des affaires).

5. Procédures de déclassification

Les dispositions qui suivent s'appliquent aux seuls informations et supports classifiés dont les délais de communicabilité prévus par le code du patrimoine ne sont pas échus et :

- qui ne comportent pas mention de la date précisant leur déclassification ;
- ou qui n'ont pas été déclassifiés avant la date d'échéance de classification.

Elles ne s'appliquent pas, par nature, aux documents déclassifiés automatiquement :

- par atteinte de l'échéance de déclassification mentionnée lors de la classification ;
- par l'atteinte du délai prévu par le code du patrimoine ou, à défaut, la date de création du document.

a. Organisation de la fonction de déclassification

L'organisation de la fonction de déclassification s'exerce selon les modalités suivantes :

Déclassification par le service auteur ou le service successeur :

La décision de déclassifier les informations et supports classifiés appartient à l'autorité émettrice qui confie cette responsabilité au service auteur. Ce dernier peut également prendre toutes les mesures justifiées visant à déclasser ou reclasser les informations et supports classifiés.

Le service auteur évalue la sensibilité des informations et supports classifiés avant de procéder éventuellement à la déclassification du document ou de l'ensemble des documents.

Lorsque le service auteur n'existe plus, la responsabilité de la décision de déclassifier, déclasser ou reclasser les informations et supports classifiés revient à un service identifié comme successeur²⁴¹ ou, à défaut, au haut fonctionnaire correspondant de défense et de sécurité.

En cas d'absence de réponse du service auteur dans les deux mois à compter de la demande de déclassification, le haut fonctionnaire correspondant de défense et de

²⁴¹ Les services héritiers sont désignés par le ministre de la défense (note n° 5158/ARM/CAB/CM1/NP du 31 juillet 2018 relative à la définition des services héritiers).

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.12**

sécurité peut évaluer lui-même la sensibilité des informations et supports classifiés et prendre la décision de les déclassifier, déclasser ou reclasser.

Documents conservés dans un service d'archives²⁴² :

Afin de simplifier et d'optimiser la bonne application de la protection du secret de la défense nationale et du code du patrimoine et de faciliter le traitement des archives publiques définitives, le SHD et l'ECPAD (pour les archives audiovisuelles) peuvent déclasser, reclasser ou déclassifier les informations et supports classifiés qui figurent dans les archives qui leurs sont confiées et qui sont émises par le ministère de la défense. Dans ce cadre, chaque décision doit être éclairée et justifiée. Elle s'appuie notamment sur les guides de classification, sur la doctrine établie par la commission de déclassification ou sur l'avis d'experts. L'ECPAD et le SHD rédigent une procédure encadrant leurs pratiques et la soumettent pour approbation à l'autorité émettrice et le fonctionnaire de sécurité et de défense.

Pour les documents relatifs à certaines thématiques revêtant une sensibilité particulière (armes nucléaires, biologiques ou chimiques, dispositifs de dissuasion, programmes d'armement encore en activité, infrastructures sensibles encore en usage), le SHD et l'ECPAD sollicitent néanmoins l'autorisation du service auteur ou successeur du ministère de la défense, ou, à défaut, du haut fonctionnaire correspondant de défense et de sécurité.

Pour les documents dont le service auteur n'est pas du ministère de la défense, le SHD et l'ECPAD s'adressent à l'autorité émettrice.

Le SHD et l'ECPAD peuvent également décider de classer tout ou partie des fonds entrés par voies extraordinaires dont ils sont dépositaires ainsi que des entretiens qu'ils peuvent être amenés à recueillir dans le cadre de leur collecte de témoignages oraux. La classification est, en effet, justifiée lorsque les fonds déposés contiennent des informations dont la divulgation est de nature à nuire à la défense et à la sécurité nationale.

Les Archives nationales et le service d'archives des Affaires étrangères peuvent solliciter la direction de la mémoire, de la culture et des archives (DMCA) pour demander la déclassification de documents conservés dans ces services lorsqu'ils émanent du ministère de la défense (cf. fiche 7.11). La DMCA sollicite alors le service auteur des documents ou son successeur, ou à défaut, le haut fonctionnaire correspondant de défense et de sécurité.

La DMCA peut saisir pour avis l'ECPAD pour la déclassification des documents audiovisuels du ministère de la défense.

En cas d'absence de réponse du service auteur dans les deux mois à compter de la demande de déclassification, le haut fonctionnaire correspondant de défense et de

²⁴² Ce paragraphe n'est pas applicable aux informations et supports classifiés *Très Secret Classification Spéciale* pour lesquels l'autorité émettrice est le Premier ministre (IGI 7.1.1.1). Le ministère n'a donc pas de marge d'appréciation sur la déclassification de ces documents (article R.2311-4 du code de la défense).

TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES TOUT AU LONG DE LEUR CYCLE DE VIE

7.12

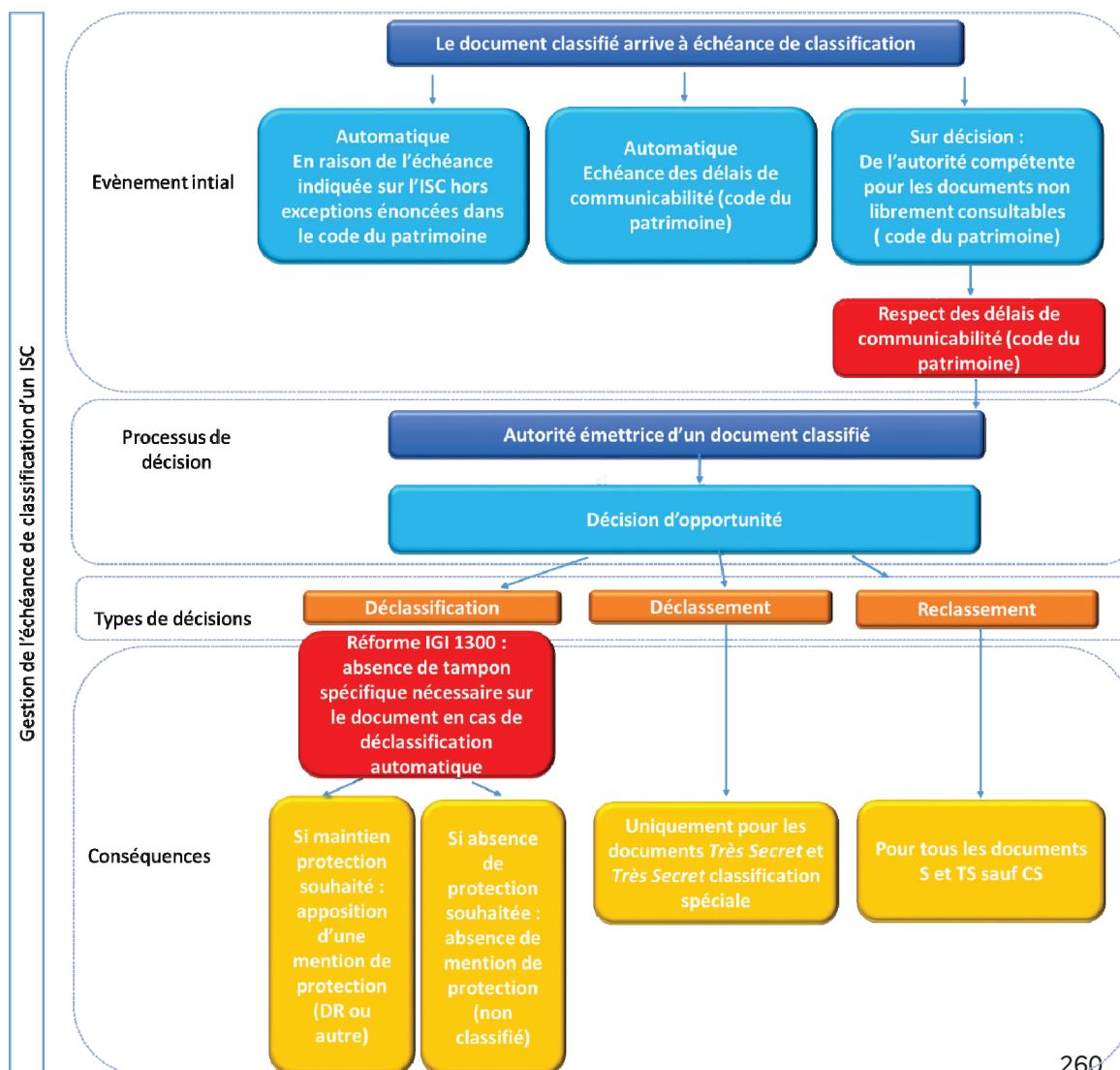
sécurité peut évaluer lui-même la sensibilité des informations et supports classifiés concernés du ministère et prendre la décision de les déclassifier, déclasser ou reclasser, à l'exception des archives étrangères.

Les décisions de déclassification sont consignées par l'organisme qui procède à la déclassification.

b. Marquage de déclassification

Le document déclassifié avant la date d'échéance ou avant l'expiration des délais de communicabilité fait obligatoirement l'objet d'un marquage de déclassification spécifique comportant la date et les références de la décision. Le document déclassé ou reclassé fait lui aussi l'objet d'un marquage analogue comportant la date et les références de la décision (cf. modèle en annexe 38 de l'IGI 1300).

Schéma de synthèse pour les documents de moins de 50 ans ou dont la date limite de classification n'est pas atteinte



**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.13****DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIÉS,
DIFFUSION RESTREINTE OU SENSIBLES****Références :**

- Code du patrimoine – articles L.212-2 et L.212-3
- IGI 1300 – 7.5.1 et 7.5.2 et annexe 45
- Arrêté du 20 août 2024 relatif aux normes techniques de destruction des informations et supports classifiés ou protégés
- Instruction n° 101/DEF/SGA/DMPA/DPC du 29 juillet 2011 relative à la politique et à l'organisation générale de l'archivage du ministère de la défense et des anciens combattants

Points clés

- La destruction est réalisée par des personnes habilitées au niveau des informations et supports classifiés.
- Après destruction des informations et supports classifiés, un procès-verbal est dressé.
- Les moyens d'impression, reproduction et de destruction des informations et supports classifiés doivent, dans la mesure du possible, être centralisés.
- Aucune destruction d'archives ne peut être réalisée sans le visa d'élimination de l'administration des archives concernée.
- De manière générale, tout document papier, même non protégé, est broyé, *a fortiori* s'il présente un caractère sensible.

1. Documents classifiés

- Les documents classifiés sont soumis à la règle commune en matière d'élimination d'archives²⁴³.

Lorsque des informations et supports classifiés sont périmés ou devenus inutiles, il est procédé à leur destruction selon les directives données par la DMCA. Afin d'établir la distinction entre les documents à détruire et ceux nécessitant une conservation, il est nécessaire de prendre contact avec le Service Historique de la Défense (SHD) (cf. [annexe 18](#)) ou l'Établissement de Communication et de Production Audiovisuelle de la Défense (ECPAD). La DMCA, le SHD ou l'ECPAD pourront délivrer, dans certains cas, des visas d'élimination par anticipation (éliminations très fréquentes de documents d'un même type).

- La destruction ne peut être réalisée que par des personnes habilitées. Il est recommandé de centraliser la destruction et la reproduction de la documentation classifiée de niveau *Secret* ou *Très Secret* chaque fois que cela est possible. Un marquage est placé sur les appareils de façon visible indiquant ceux conformes pour ces opérations. Des signalisations indiquant le niveau maximum autorisé de

²⁴³ Cf. instruction de référence.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.13**

sensibilité ou de classification des documents sont placées sur chaque appareil pour la destruction, l'impression et la reproduction. La destruction des informations et supports classifiés est effectuée de façon à rendre impossible toute reconstitution, même partielle, des informations contenues sur les supports. Les principales formes de destruction sont :

- l'incinération ou le brûlage²⁴⁴ ;
- le broyage ;
- le déchiquetage ;
- la surtension électrique²⁴⁵ ;
- l'immersion dans un bain d'acide.

Lorsque des documents classifiés doivent être transportés afin d'être incinérés, ils doivent impérativement avoir été préalablement déchiquetés et mélangés.

- Nouvelles modalités liées à l'arrêté cité en référence : le choix de la modalité de destruction des informations et supports classifiés dépend du degré de destruction défini et associé à chaque type de support.
- Après l'opération, un procès-verbal de destruction est dressé. Ce procès-verbal de destruction porte la signature du détenteur et, pour les documents *Très Secret*, celle d'un témoin habilité au niveau *Très Secret*. Les modèles de procès-verbal figurent en annexe 45 de l'IGI 1300. Ceux-ci sont conservés pendant cinq ans par le détenteur et l'officier de sécurité de l'organisme.
- Au niveau *Très Secret*, le détenteur du document sollicite officiellement (cf. annexe 18) l'autorité émettrice et lui rend compte, sauf avis contraire de sa part, qu'il procédera à la destruction du support. Sans réponse dans un délai de deux mois, le service détenteur procède à la destruction du support et en rend compte à l'autorité émettrice en lui adressant une copie du procès-verbal²⁴⁶. Une copie de ce procès-verbal est également transmise au bureau de protection du secret. Cette procédure n'est pas requise pour le niveau *Secret*.
- Tout support de stockage électronique classifié mis au rebut est préalablement effacé selon des procédés employant des produits certifiés ou qualifiés par l'ANSSI pour l'effacement (par exemple, un produit d'effacement sécurisé pour la mention *Diffusion Restreinte*). Le support électronique est ensuite détruit physiquement, selon un procédé qui rend impossible la reconstitution de tout ou partie de l'information classifiée ou sensible contenue sur ce support (si possible conforme aux recommandations du SGDSN).

²⁴⁴ L'incinération consiste à réduire l'information ou le support classifié en cendres, le brûlage pour sa part est l'incinération incomplète qui ne permet pas de reconstituer ou de prendre connaissance de l'information.

²⁴⁵ Les normes techniques sont arrêtées par le SGDSN, après expertise des services compétents.

²⁴⁶ En cas de dissolution du service dont relevait l'autorité ayant procédé à la classification, la copie du procès-verbal de destruction est adressée au S-HFDS du ministère compétent.

**TITRE 7 : SECURITE DES INFORMATIONS ET SUPPORTS CLASSIFIES
TOUT AU LONG DE LEUR CYCLE DE VIE****7.13****2. Informations *Diffusion Restreinte* ou sensibles**

Par prudence, tous les documents papier considérés comme sensibles ainsi que ceux portant la mention de protection *Diffusion Restreinte* ou une mention de confidentialité spécifique doivent recevoir le traitement suivant :

- tous les supports papier sont jetés dans une corbeille à papier, distincte de la poubelle de bureau, laquelle n'est destinée qu'à recueillir des déchets ;
- ces corbeilles seront vidées chaque soir par leur détenteur et leur contenu broyé (les broyeurs existants, destinés aux informations et supports classifiés, peuvent être utilisés).

Ces dispositions permettent de réduire le risque de *TrashInt* (*Trash Intelligence*), qui renvoie à un procédé d'espionnage réalisé par l'analyse d'informations sensibles recueillies dans les corbeilles à papier des organismes.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.14****ÉVACUATION ET DESTRUCTION D'URGENCE****Référence :**

- IGI 1300 – 7.5.3

Points clés

- Pour faire face à des circonstances exceptionnelles, l'organisation d'une éventuelle évacuation ou destruction d'urgence est planifiée en amont.
- Lors de la rédaction des plans afférents, il est nécessaire de prendre en compte le volume des informations et supports classifiés à transporter ou à détruire.

1. Plan d'évacuation et de destruction d'urgence

Pour faire face à des circonstances exceptionnelles et en cas de menace immédiate nécessitant l'évacuation des bâtiments par le personnel ou la destruction des informations et supports classifiés, des plans d'évacuation et de destruction d'urgence sont établis par chaque service ou entité qui détient des informations et supports classifiés. Ces plans prévoient notamment les procédures d'accès, en toute circonstance, aux locaux et donc aux informations et supports classifiés

Les modalités pratiques d'exécution de ces plans figurent sur des fiches placées dans chaque coffre contenant des informations et supports classifiés. Elles précisent :

- les autorités désignées pour donner l'ordre de destruction ou d'évacuation ;
- la liste des personnes pouvant accéder aux locaux et ouvrir les meubles de sécurité pendant et hors heures ouvrables ;
- la liste et la localisation des informations et supports classifiés et des articles contrôlés de la sécurité des systèmes d'information à détruire ou à évacuer ;
- les mesures applicables aux systèmes d'information ;
- la liste et la localisation des moyens de destruction et d'évacuation à utiliser.

La mise en œuvre du dispositif ainsi établi est contrôlée au minimum tous les trois ans par l'officier de sécurité de l'organisme. Ce contrôle fait l'objet d'un compte-rendu diffusé aux personnes concernées, il précise les points qui doivent être modifiés. Il est conservé par l'officier de sécurité de l'organisme concerné.

2. Ordre de destruction ou d'évacuation d'urgence

L'ordre de destruction ou d'évacuation d'urgence est transmis suivant les cas par :

- note écrite (ou message) revêtue de la signature de l'autorité désignée ;
- téléphone : dans ce cas, l'ordre est authentifié par rappel de l'autorité désignée pour donner l'ordre de destruction ou par tout autre moyen permettant de s'assurer de la réalité de l'ordre donné. Dans la mesure du possible, l'ordre téléphoné est suivi d'une note ou d'un message ;
- de vive voix, par l'autorité désignée ou l'officier de permanence ou assimilé, notamment en cas de catastrophe naturelle.

**TITRE 7 : SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS
TOUT AU LONG DE LEUR CYCLE DE VIE****7.14**

Dans la mesure du possible, les cahiers d'enregistrement, les procès-verbaux d'inventaires, de destruction, les fiches de position des documents sont conservées.

Après application des directives, il est procédé à :

- un procès-verbal de destruction ;
- un compte-rendu d'exécution.

Ces documents sont adressés à l'officier de sécurité et au bureau de protection du secret de l'entité.

TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA DÉFENSE NATIONALE

INTRODUCTION : GÉNÉRALITES

Références :

- Code de justice militaire – article L.332-2
- Code pénal – articles 121-2, 413-9 à 413-14, 414-7 à 414-9
- IGI 1300 – 1.2.2.2, 1.4.1 et 1.4.2
- II n° 500 bis/SGDN/TTS/SSI/DR du 18 octobre 1996 relative au chiffre dans la sécurité des systèmes d'information
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information
- IM n° 7326/DEF/CAB du 25 juin 2018 relative à la politique de sécurité du système d'information du ministère de la défense (PSSI-M)
- Directive n° 485/SGDN/TTS/SSI du 20 novembre 2013 relative à l'installation des sites et systèmes d'information pour la protection contre les signaux parasites compromettants

Point clé :

La compromission se caractérise par l'accès à une information ou un support classifié d'une personne non habilitée ou qui ne dispose pas du besoin d'en connaître. Elle peut être intentionnelle ou non intentionnelle.

1. Définition

La compromission se définit comme la destruction, le détournement, la soustraction ou la reproduction non autorisée d'une information ou d'un support classifié ainsi que le fait de divulguer ou de rendre possible la divulgation d'un secret de la défense nationale. Il convient de considérer que la compromission est possible dès qu'une information ou un support classifié a échappé au contrôle continu de la personne qui assure sa protection. Le compte-rendu de cette dernière est immédiat.

Les sanctions pénales encourues sont décrites aux articles 413-10 à 11 du code pénal.

Outre des sanctions pénales, l'auteur d'un acte, commis délibérément ou non, qui compromet un secret de la défense nationale, encourt l'abrogation de sa décision d'habilitation, la révision de son avis de sécurité ainsi que des sanctions administratives et disciplinaires.

Les personnes morales sont pénalement responsables des faits de compromission qui leur sont imputables et encourrent, outre une peine d'amende, l'interdiction d'exercer dans le domaine d'activité dans lequel l'infraction a été commise.

TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA DÉFENSE NATIONALE

2. Indices révélateurs d'une compromission

Outre le vol, la disparition ou la perte de contrôle de l'information ou du support classifié, une compromission peut être révélée par :

- un incident réel ou supposé d'un système numérique ou de la découverte d'un piégeage pouvant remettre en cause la confidentialité d'une information (II 910) ;
- la modification non autorisée d'un élément de protection d'un système numérique (directive 911) ;
- un incident ou accident affectant un système numérique classifié de défense (IM 133) ;
- une exploitation de signaux électromagnétiques compromettants (directive 485, guide 960) ;
- la pénétration dans des lieux abritant ou des locaux techniques ou la détention d'un moyen pouvant contribuer à la fuite d'informations (téléphones portables par exemple).

**TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA
DÉFENSE NATIONALE****8.1****TRAITEMENT DES COMPROMISSIONS****Référence :**

- Code pénal – article 434-4
- IGI 1300 – 1.4.2.3
- IM 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées (PSSI-M)

Points clés

- La compromission se caractérise par l'accès à une information ou un support classifié d'une personne non habilitée ou qui ne dispose pas du besoin d'en connaître. Elle peut être intentionnelle ou non intentionnelle.
- En cas de suspicion de compromission, le responsable d'organisme prend sans délai toute mesure conservatoire et informe le service enquêteur, qui effectue une investigation et analyse les faits.
- Si le doute n'est pas levé sur la compromission, le service enquêteur informe et transmet les éléments à la Direction générale de la sécurité intérieure (DGSI) pour enquête.

La rapidité et la discrétion de l'intervention revêtent une importance primordiale pour limiter les conséquences de la divulgation des informations et supports classifiés compromis.

La suspicion de compromission est le terme à employer lorsque la divulgation d'informations et supports classifiés a été rendue possible.

La compromission avérée signifie qu'il est établi qu'une information ou un support classifié a été porté à la connaissance d'une personne non qualifiée.

1. Action de l'autorité hiérarchique

Dès qu'une personne d'un organisme découvre une compromission possible, il rend compte immédiatement à son autorité hiérarchique et à son officier de sécurité (qui, si nécessaire, se coordonne avec l'officier de sécurité des systèmes d'information).

Lorsqu'une compromission est avérée ou lorsqu'il s'agit d'une suspicion de compromission, le responsable d'organisme se conforme en tout point à la procédure décrite ci-dessous.

Le responsable d'organisme veille à faire prendre les mesures conservatoires appropriées et à informer le service enquêteur. En liaison étroite avec ce dernier, les mesures suivantes sont appliquées :

**TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA
DEFENSE NATIONALE****8.1**

- Pour les états-majors, directions et services uniquement, un message « FLASHEVENT », est adressé à :
 - o pour action : au Cabinet du ministre (CAB/BRES), à la DPID, aux autorités hiérarchiques à laquelle l'unité est rattachée, à la DRSD, la DGSE si son domaine de compétence est concerné et à l'officier de sécurité de niveau 1,
 - o pour information : au service de la DRSD localement compétent (poste et direction zonale concernée), au délégué d'armée représentant local de l'armée considérée,
 - o dans tous les cas : ces dispositions s'appliquent également aux cas de compromissions et de divulgations d'informations et supports classifiés étrangers détenus par la France (cf. fiche 8.3) du fait :
 1. de sa coopération avec les États de l'Alliance atlantique et de l'UE,
 2. d'accords de sécurité bilatéraux conclus avec des États qui ne sont membres ni de l'une ni de l'autre de ces deux organisations et d'accords portant sur les informations et supports classifiés échangés avec des organisations internationales.
- Pour tous (états-majors, directions et services et personnes morales contractantes) : un compte-rendu détaillé dans les trente jours.
- Le délai est impérativement respecté même si tous les éléments n'ont pas pu être apportés. Ils sont adressés par la suite dans un message complémentaire. Concernant les établissements publics, le service de la DRSD compétent doit être immédiatement informé. La DRSD informe la direction de tutelle, le cabinet du ministre et le HFCDS.

Pour les personnes morales sous contrat ou convention : un compte-rendu immédiat est envoyé à la DRSD, copie DGA/SSDI. La DRSD retransmet ce compte-rendu dans les plus brefs délais au cabinet du ministre (CAB/BRES) et au HFCDS.

Le compte-rendu détaillé à 30 jours peut être classifié, si nécessaire, selon les modalités de transport définies dans le titre 7.

En cas de compromission avérée ou de suspicion de compromission, le chef de cabinet militaire du ministre, en tant que HFCDS, informe le SGDSN.

Lors d'une mission effectuée en isolé (personne seule ou en petit groupe) à l'étranger, en cas de perte ou de vol d'informations et supports classifiés, il convient de prévenir le plus rapidement l'ambassade de France ou le consulat, de rendre compte à sa hiérarchie, civile ou militaire et, selon les directives reçues, d'informer les autorités de police du pays.

2. Préservation des preuves et investigation

Des mesures de préservation de l'objet, du système ou des traces nécessaires à l'enquête doivent être prises dès que possible. Ces mesures conservatoires font l'objet de l'annexe 19. Il est toutefois rappelé que toute investigation ou action, quelle qu'elle soit, susceptible de modifier ou détruire des éléments de preuve et de compromettre la valeur des traces informatiques est formellement proscrite. La non-observation de

TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA DEFENSE NATIONALE

8.1

cette règle est susceptible d'exposer le responsable de l'action menée à des sanctions pénales (article 434-4 du code pénal).

Dans certains cas (atteinte d'un serveur ou d'un élément actif d'un réseau par exemple), les nécessités de l'enquête peuvent conduire à suspendre le fonctionnement du système numérique (IM 7326-2). Il appartient aux responsables de ce dernier de prévoir et d'adopter des solutions de secours permettant d'assurer à cette occasion une continuité de service adaptée (II 500 bis). Les mesures correspondantes doivent être décrites dans la procédure d'exploitation de sécurité du système.

Tous les éléments recueillis sont mis à la disposition de la DRSD, dans les plus brefs délais, pour la conduite de son enquête.

3. Action du service enquêteur

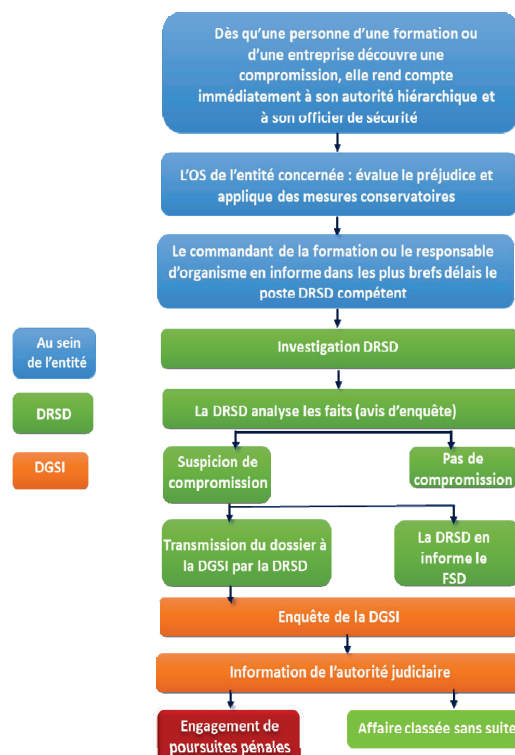
La DRSD est le service du ministère de la défense compétent pour le traitement des compromissions, à l'exclusion du périmètre de compétence de la DGSE. À ce titre, elle est sollicitée dès que des indices sont constatés, notamment :

- dégradations d'emballage contenant des informations et supports classifiés ;
- disparition, définitive ou temporaire, partielle ou totale de supports susceptibles de contenir des informations et supports classifiés ;
- traces d'effraction dans un lieu abritant ;
- découverte d'un dispositif illicite permettant de recueillir ou d'accéder à des informations et supports classifiés.

Informé par le responsable d'organisme concerné par une compromission avérée ou une suspicion de compromission, le représentant de la DRSD, après avoir procédé aux investigations nécessaires, rédige un compte-rendu immédiat.

Lorsque les investigations confirment la suspicion ou la compromission, la DRSD, après avoir informé le responsable de l'organisme concerné et la chaîne des officiers de sécurité, transmet le dossier à la DGSI (ou à la gendarmerie prévôtale sur les théâtres d'opérations extérieures ou en zone de stationnement des forces françaises), qui procède à l'enquête judiciaire.

La DRSD en informe le fonctionnaire de sécurité et de défense.



**TITRE 8 : GESTION ET REPRESSION DES ATTEINTES AU SECRET DE LA
DEFENSE NATIONALE****8.1**

Les organismes liés au ministère de la défense ou au CEA/DAM par contrat ou par convention saisissent l'entité DRSD compétente, qui rend compte à son tour à sa direction centrale. Cette dernière informe l'autorité contractante (DGA, par exemple).

**TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA
DÉFENSE NATIONALE****8.2****COMPROMISSION AFFECTANT UN SYSTÈME NUMÉRIQUE****Référence :**

- IGI 1300 – 1.4.2.4

Points clés

- Tout support informatique potentiellement affecté par une compromission cesse d'être utilisé et est conservé dans un endroit sécurisé.
- L'officier de sécurité et l'officier de sécurité des systèmes d'information sont les acteurs agissant dans la mise en œuvre de la procédure.
- Le service enquêteur est saisi et procède aux investigations en liaison avec l'ANSSI avant transmission éventuelle à la DGSI.

La présente fiche complète la fiche 8.1 dans le cas où la compromission (cf. définition de la fiche 8.1, §1) concerne un système numérique, qu'il s'agisse d'une suspicion de compromission ou d'une compromission avérée. Les dispositions prévues par la fiche 8.1 de la présente instruction sont applicables (« FLASHEVENT », etc.).

1. Réactions immédiates

Il convient de :

- préserver le support numérique susceptible d'être affecté par une compromission (cesser de l'utiliser par exemple) ;
- saisir l'officier de sécurité, qui saisit l'officier de sécurité des systèmes d'Information ainsi que le service enquêteur qui prend en charge les investigations et informe l'ANSSI ;
- le cas échéant, pour les états-majors, directions et services : informer l'officier de sécurité du Commissariat au Numérique de Défense (CND) ;
- rassembler les éléments techniques et humains en rapport avec l'incident en cours²⁴⁷.

Dans le cas où les services spécialisés du Commissariat au Numérique de Défense (CND) découvrent qu'un système numérique est affecté par une compromission, ils doivent saisir le service enquêteur et l'officier de sécurité de l'organisme concerné qui est alors responsable de conduire les actions relatives à cette compromission.

Toutes les actions entreprises entrent dans le cadre d'une première réponse sur incident. Elles doivent impérativement être répertoriées et horodatées dans un registre dédié.

²⁴⁷ Pour préserver la validité de futures investigations judiciaires, les éléments de preuve (messages, documents, etc.) ne doivent pas être effacés mais conservés dans des fichiers spécifiques ou à défaut sur un support classifié dédié à cette conservation. L'officier de sécurité et l'officier de sécurité des systèmes d'information doivent conserver la trace de leurs actions visant à faire cesser au plus vite la compromission.

**TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA
DÉFENSE NATIONALE****8.2**

L'officier de sécurité des systèmes d'information de l'organisme concerné prend toutes les mesures nécessaires pour garantir la sauvegarde et l'intégrité des preuves techniques. Toute intervention de personnel non qualifié (visualisation du contenu d'un message, fichier ou répertoire, etc.) sur la machine est de nature à laisser des traces sur le disque dur et ainsi à rendre la preuve judiciairement irrecevable. Seules des interventions justifiées par l'état de nécessité sont autorisées.

2. Règles de base applicables par l'organisme touché par une compromission possible à la charge de l'officier de sécurité des systèmes d'information ou officier de sécurité**a. Suspicion de compromission sur une machine isolée**

- Si l'équipement est en fonctionnement :
 - o laisser la machine en fonctionnement,
 - o ne pas retirer les médias amovibles connectés, s'il y en a.
- Si l'équipement a été éteint : ne pas rallumer la machine.
- Si la machine est reliée à un serveur de stockage : appliquer les consignes *supra* au serveur.

b. Suspicion de compromission sur une machine connectée au réseau

Appliquer les mêmes dispositions que celles prévues pour une machine isolée.

En complément :

- noter le numéro de la prise murale du réseau ;
- débrancher le câble réseau ;
- demander aux administrateurs du système de mettre à disposition du service enquêteur les journaux d'événements des différents équipements liés (serveurs, commutateurs, etc.).

3. Premières constatations et investigations

Au-delà des règles de base précisées *supra*, les premières constatations et les investigations ultérieures doivent être réalisées par le service enquêteur dès qu'une suspicion de compromission affectant un système numérique est signalée.

**TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA
DÉFENSE NATIONALE****8.3****COMPROMISSION D'INFORMATIONS CLASSIFIÉES ÉTRANGÈRES****Références :**

- Code pénal – articles 414-8 et 414-9
- IGI 1300 – 1.4.2.3
- II n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI)

Points clés

- Les faits de compromission d'informations et supports classifiés étrangers doivent être signalés à l'autorité de sécurité déléguée compétente ou à l'autorité nationale de sécurité.
- Il convient de bien distinguer les informations et supports classifiés nationaux des informations et supports classifiés étrangers dans l'armoire forte.

Lorsqu'une suspicion de compromission ou compromission avérée porte sur des informations et supports classifiés d'origine étrangère (ou sur des informations et supports classifiés communs partagés dans le cadre de programmes ou projets en coopération), et sans préjudice des dispositions mentionnées aux fiches 8.1 et 8.2 de la présente instruction, les mesures suivantes s'appliquent, sous réserve des dispositions de l'accord de sécurité conclu avec l'État correspondant :

- le détenteur rend compte le plus rapidement possible à l'officier de sécurité compétent (cf. fiche 9.1). Sur le territoire national, lorsque l'autorité de sécurité déléguée est saisie, elle informe le service enquêteur compétent (en charge de caractériser la compromission) et le SGDSN de la constatation d'une compromission possible d'informations et supports classifiés et des mesures immédiates prises ;
- pour les compromissions sur des informations et supports classifiés de niveau *Très Secret* ou équivalent, le SGDSN assure seul la relation avec les autorités de sécurité étrangères, sur la base, le cas échéant, du compte-rendu adressé dans les meilleurs délais par l'autorité de sécurité déléguée française compétente ;
- pour les compromissions des informations et supports classifiés jusqu'au niveau *Secret* ou équivalent (ce qui peut inclure le niveau *Diffusion Restreinte* au sens des accords et règlements de sécurité internationaux), l'autorité de sécurité déléguée (ou à défaut l'ANS) informe, le plus rapidement possible, le pays d'origine de l'information (ou le pays partenaire en cas de projet/programme en coopération) de la compromission avérée ou suspectée. Un rapport d'enquête final rédigé par le service enquêteur est transmis aux autorités étrangères via l'ANS ou l'ASD au plus tard 31 jours ouvrables après le constat avéré de la compromission ;
- pour les compromissions touchant aux articles contrôlés de la sécurité des systèmes d'information étrangers, le Commissariat au Numérique de Défense (CND) coordonne la remontée d'informations vers les autorités de sécurité étrangères avec la chaîne de sécurité afin de préserver la cohérence de l'action du ministère de la défense et d'assurer l'information du service enquêteur du ministère.

**TITRE 8 : GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA
DÉFENSE NATIONALE****8.3**

Afin d'éviter le risque de compromission d'informations étrangères et, sauf dispositions contraires prévues par l'accord de sécurité ou définies par les autorités de sécurité compétentes des parties concernées, les documents d'origine étrangère sont marqués au moins sur la première page, selon le timbre équivalent français.

Ces dispositions sont applicables aux actes commis au préjudice :

- des puissances signataires de l'OTAN ou d'une institution ou d'un organe de l'OTAN²⁴⁸ ;
- d'un État étranger ou d'une organisation internationale en vertu d'un accord de sécurité, régulièrement approuvé et publié, relatif à la protection des informations et supports classifiés conclu entre la France et un État étranger ou une organisation internationale ;
- d'une institution, d'un organe ou d'un organisme de l'UE en vertu des règles de sécurité de ces derniers qui ont fait l'objet d'une publication au Journal officiel de l'Union européenne²⁴⁹.

À titre d'information, pour connaître toute équivalence, il y a lieu de consulter les accords ou règlements de sécurité des principales organisations internationales dont la France fait partie ou l'accord de sécurité avec le pays considéré et à défaut, de prendre contact avec le bureau DIE de la DAJ. Des équivalences spécifiques, dérogoires aux tables d'équivalences de classification des accords ou règlements de sécurité peuvent également avoir été mises en place au sein d'un programme, d'un projet ou d'un contrat donné. De telles équivalences spécifiques sont mises en place par l'autorité nationale de sécurité ou par l'autorité de sécurité déléguée, en lien avec l'État étranger ou l'organisation internationale, et spécifiées dans des textes appropriés qui doivent faire partie du référentiel applicable du programme, du projet ou du contrat.

Enfin, les documents classifiés relevant d'une organisation internationale sont conservés dans des meubles de sécurité, ou coffres, séparément des documents classifiés nationaux ou étrangers, afin de ne pas compromettre l'information nationale ou étrangère lors d'une inspection éventuelle des organismes de contrôle de ces organisations (respect du principe du besoin d'en connaître – cf. fiches 7.10 et 9.4).

²⁴⁸ Article 414-8 du code pénal.

²⁴⁹ Article 414-9 du code pénal.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

INTRODUCTION : PRINCIPES DE LA PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

La fiche 1 précise les responsabilités du secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité nationale de sécurité (ANS), relatives à la protection du secret dans les relations internationales ainsi que celles des autorités de sécurité déléguée (ASD), en particulier celles de la Direction générale de l'armement (DGA), en tant qu'autorité de sécurité déléguée dans le domaine de l'industrie de défense tel que spécifié dans la note de délégation du SGDSN.

Les fiches 2 à 5 établissent les règles de protection des informations et supports classifiés, *Diffusion Restreinte* ou sensibles à observer par les agents des services étatiques du ministère de la défense, des organismes et écoles sous sa tutelle et de l'industrie de défense, dans le cadre des échanges internationaux, des missions accomplies à l'étranger en dehors des opérations, des visites en France de personnel étranger.

Elles précisent également les dispositions à prendre dans le cadre d'accords avec les organisations internationales (OTAN, OCCAr, UE, EDIR/FA)²⁵⁰.

Les dispositions spécifiques relatives à la protection du potentiel scientifique et technique de la Nation, définies dans le décret n°2011-1425 du 2 novembre 2011, ne sont pas traitées dans cette instruction²⁵¹.

Enfin, la fiche 6 traite des missions et séjours à l'étranger. Dans ce domaine, il est crucial d'intégrer que le contexte international géopolitique et économique actuel de montée des tensions peut accroître les vulnérabilités des personnes morales et physiques. Il incombe à tous les acteurs – militaires et civils de la défense, officiers de sécurité, chefs d'organisme, etc. d'appliquer la réglementation et d'accomplir ces missions avec la plus grande rigueur et vigilance.

²⁵⁰ Organisation du Traité de l'Atlantique Nord, Organisation conjointe de coopération en matière d'armement, Union européenne, *European Defense Industry Restructuring/Framework Agreement*.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.1****AUTORITÉ NATIONALE DE SÉCURITÉ ET AUTORITÉ DE SÉCURITÉ DÉLÉGUÉE****Références :**

- IGI 1300 - 2.1.1.2.b
- Code de la défense - articles R.2311-10 à R.2311-11

Points clés

- Le secrétaire général de la défense et de la sécurité nationale est l'autorité nationale de sécurité en matière de protection du secret. À ce titre, il est le seul responsable de la négociation et de la conclusion des traités et accords intergouvernementaux en matière d'échange et de protection réciproque des informations et supports classifiés, qui ne sont pas limités à un domaine donné et appelés aussi accords généraux de sécurité (AGS).
- La direction générale de l'armement (DGA) est l'autorité de sécurité déléguée (ASD) par le SGDSN dans le domaine de l'industrie de défense tel que spécifié par le SGDSN. La DGA informe le service du HFCDS des dispositions prises et s'appuie, autant que de besoin, sur la direction des affaires juridiques du ministère. Elle apporte son soutien et son expertise au SGDSN pour la rédaction et la négociation des accords de sécurité qui encadrent des coopérations ou des exportations en matière d'armement. En appui du SGDSN, elle est une interlocutrice des autorités nationale de sécurité et autorités de sécurité déléguée étrangères pour la mise en œuvre des dispositions des accords de sécurité bilatéraux ou conclus avec les organisations internationales, la définition des mesures de protection à apporter aux informations et supports classifiés échangés lors des coopérations ou des exportations en matière d'armement, l'échange d'informations sur les habilitations de sociétés ou de personnes et la mise en œuvre des processus et règles en matière de sécurité industrielle internationale, définies par les accords ou les documents de sécurité complétant ces accords.
- D'autres autorités de sécurité déléguée peuvent être désignées par le SGDSN.

1. Autorité nationale de sécurité

L'autorité nationale de sécurité est, pour le secret de la défense nationale, l'entité gouvernementale interministérielle chargée des relations avec les autres États et les structures internationales en matière d'habilitation de personnes et de protection des informations et supports classifiés. En France, l'autorité nationale de sécurité est le **secrétaire général de la défense et de la sécurité nationale**.

L'**agence nationale de la sécurité des systèmes d'information (ANSSI)**, service à compétence nationale rattaché au SGDSN, est l'autorité nationale de défense et de sécurité des systèmes d'information. Elle est chargée d'assister le SGDSN pour l'exercice de ses attributions.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

9.1

2. Autorité de sécurité déléguée²⁵²

L'autorité de sécurité déléguée est l'autorité responsable devant l'autorité nationale de sécurité de la mise en œuvre de la politique de sécurité du secret de la défense nationale dans un domaine particulier. Elle est désignée par l'autorité nationale de sécurité (SGDSN) sur proposition du ministre. Au sein du ministère de la défense, la **DGA** est l'autorité de sécurité déléguée dans le domaine de l'industrie de défense.

La DGA en tant qu'autorité de sécurité déléguée est chargée dans son domaine de compétence :

1/ d'instruire les demandes d'habilitation en relation avec les autorités de sécurité nationales ou autorités de sécurité déléguées étrangères, dans le cadre de l'application des accords de sécurité et des règlements de sécurité internationaux conclus avec la France et notamment :

- de saisir les ANS ou ASD étrangères aux fins d'habilitation d'entreprises étrangères lorsque ces entreprises participent à des contrats passés par le ministère de la défense ou en sous-traitance de ces contrats ;
- d'instruire, à la demande d'une ANS ou ASD étrangère, les demandes d'habilitation d'entreprises françaises lorsque celles-ci participent à des contrats passés dans le pays dont relève cette ANS ou ASD ;
- d'instruire les demandes d'habilitation de personnes morales françaises candidates à un contrat impliquant l'accès à des informations classifiées de l'OTAN ou de l'Union européenne, en application du règlement de sécurité de l'Alliance atlantique ou de règlements de sécurité de l'UE ainsi que les personnes physiques impliquées dans ces contrats ;
- d'instruire, sur la base d'un avis de sécurité obtenu, le cas échéant, auprès des autorités de sécurité étrangères par le SGDSN, les dossiers d'habilitations du personnel étranger des entreprises françaises habilitées par le ministère de la défense jusqu'au niveau *Très Secret* inclus, en traitant directement avec :
 - o les autorités de sécurité étrangères pour les ressortissants des pays-membres de la communauté *EDIR/FA* (*European Defense Industry Restructuring / Framework Agreement*) ou de l'*OCCAR* (*Organisation Conjointe de Coopération en matière d'Armement*),
 - o les autorités de sécurité étrangères pour les ressortissants des pays non membres de la communauté *EDIR/FA* ou de l'*OCCAR*, après accord formel du SGDSN.

2/ d'établir les autres actes administratifs relevant de la sécurité industrielle internationale et notamment :

- délivrer les certificats de courrier ;
- traiter et approuver des plans de transport ;
- traiter et approuver les demandes de visite, de et vers l'étranger.

²⁵² En anglais : DSA (*Designated Security Authority*).

**TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS
INTERNATIONALES****9.1**

3/ d'être l'interlocuteur direct des ANS et ASD étrangères dans la définition des mesures de protection à apporter aux informations et supports classifiés traités dans un environnement multinational et notamment :

- de participer à la rédaction des instructions de sécurité programme dans le cadre des programmes en coopération, de les accepter et de vérifier leur application ;
- de traiter les plans contractuels de sécurité liés à un contrat dépassant le cadre strictement national, dénommés *Security Aspect Letters (SAL)* ;
- de traiter les cas de compromissions selon les dispositions de l'IGI 1300.

4/ de participer, lorsque l'accord de sécurité le prévoit, aux contrôles effectués pour vérifier la bonne exécution des mesures de sécurité, en coordination avec le service enquêteur du ministère de la défense.

5/ de représenter la France, seule ou en soutien du SGDSN, dans les enceintes multinationales traitant des questions de sécurité industrielle.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.2****CONDITIONS POUR ÉCHANGER DES INFORMATIONS ET SUPPORTS CLASSIFIÉS AVEC L'ÉTRANGER****Références :**

- IGI 1300 – 4.4.1.4.f, 4.4.1.4.g et 7.2.1.3
- II n° 50/SGDN/SSD/DR du 9 janvier 1971 sur la protection du secret dans les rapports entre la France et les États étrangers

Points clés

- Les échanges d'informations et supports classifiés avec l'étranger se font sur la base d'un accord de sécurité signé entre les gouvernements des deux États.
- Les accords de sécurité définissent les équivalences des niveaux de protection dans chacun des pays et instaurent la réciprocité de la protection des informations et supports classifiés.
- Le SGDSN pilote la négociation des accords généraux de sécurité (AGS).
- La direction des affaires juridiques (DAJ) pilote la rédaction et la négociation des accords de sécurité dans le domaine de la défense (ASDD) au ministère, en lien avec le SGDSN. Quand ces accords encadrent des coopérations ou des exportations d'armement, l'autorité de sécurité déléguée (la DGA, au sein de laquelle cette compétence est exercée par SSDI) participe à la négociation.

1. Règlementation et dispositions préalables

Une information classifiée ne peut être communiquée à un gouvernement étranger ou à l'un de ses ressortissants que dans le cadre d'un accord de sécurité signé entre le gouvernement de cet État et le gouvernement de la République française. Plusieurs types d'accords peuvent être conclus en fonction de la nature des échanges d'informations et supports classifiés :

- accords généraux de sécurité applicables à tous les ministères ;
- accords de sécurité dans le domaine de la défense ou d'armement, applicables au seul ministère.

En l'absence des accords de sécurité mentionnés ci-avant, peuvent également être mis en place, à titre exceptionnel, des accords intergouvernementaux sous forme d'échange de notes verbales ou par des dispositions particulières de sécurité signées par les ministres applicables à un projet particulier et généralement pour la seule transmission d'informations et supports classifiés vers le pays demandeur.

Pour l'exécution d'une coopération dans un domaine donné (programme d'armement, coopérations militaires ou industrielles) ou d'une opération d'exportation, d'autres clauses dans les accords relatifs à cette coopération et dans les contrats qui en résultent ou des documents spécifiques (instruction de sécurité programme) peuvent compléter ou décliner les dispositions de sécurité des accords de sécurité.

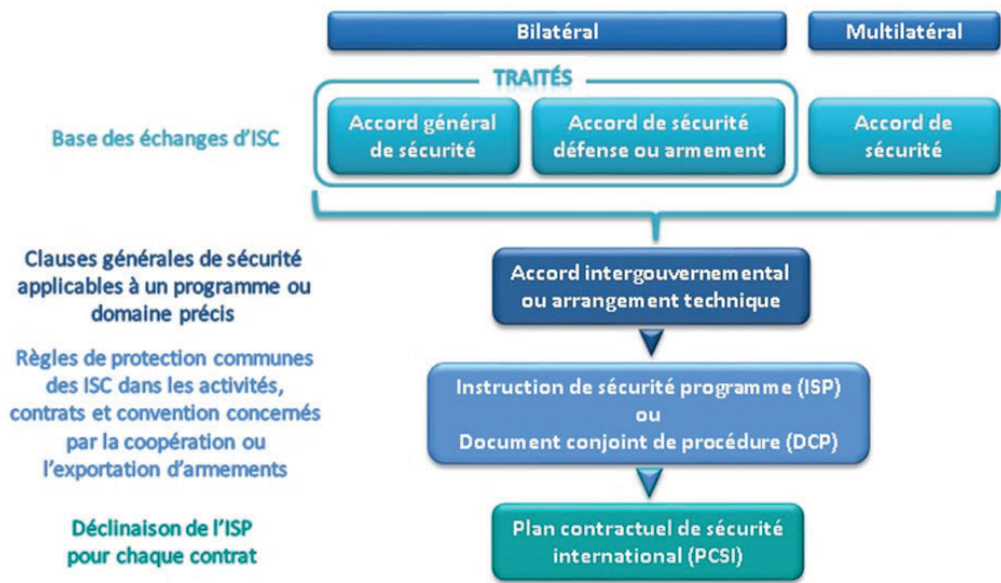
Si la communication doit intervenir dans le cadre d'une organisation internationale (OI), il convient de se référer aux textes de sécurité régissant ladite organisation. Pour l'exécution d'une coopération dans un domaine donné (programme d'armement, coopérations militaires ou industrielles), d'autres clauses ou documents peuvent

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES

9.2

compléter les dispositions de sécurité dans les accords inter gouvernementaux relatifs à cette coopération avec l’organisation internationale et dans les contrats qui en résultent ou dans des documents spécifiques (instruction de sécurité programme).

2. Les différents documents traitant d’informations et supports classifiés à l’international



Une description détaillée du contenu et de la portée des documents présentés ci-dessous figure en annexe 20.

BESOIN	DOCUMENT
Engagement réciproque de deux gouvernements, dans le domaine général ou un domaine particulier	Accord Général de Sécurité Accord de sécurité dans un domaine spécifique (par exemple celui de l'armement ou de la défense) Accord par échanges de lettre ou de notes
Échange de lettres entre ministres engageant le ministère de la défense rédigeant la réponse pour une affaire ou un programme particulier	Dispositions particulières de sécurité
Lettre engageant une autorité de sécurité pour une affaire ou un programme particulier	Assurance de sécurité s'appliquant dans un cadre OTAN ou OCCAR
Programme Coopération étatique	Accord intergouvernemental ou arrangement technique ou administratif Clause de non divulgation - Non Disclosure Agreement/Arrangement (NDA) Instruction de sécurité programme (ISP) Plan contractuel de sécurité international (PCSI)

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES
9.2

BESOIN	DOCUMENT
Programme Coopération étatique impliquant des industriels	Instruction de sécurité programme Plan contractuel de sécurité international ou Security Aspect Letter lorsque l'Etat étranger adresse des informations et supports classifiés à la France
Vente d'armements à l'export entre un industriel français et un État étranger	Instruction de sécurité programme (ISP) le cas échéant Plan contractuel de sécurité international (PCSI) Clause de non divulgation - Non Disclosure Agreement (NDA)
Sous-traitance entre la France et l'étranger (et vice versa) entre un industriel français et un industriel étranger	Plan contractuel de sécurité international ou Security Aspect Letter (SAL) lorsque un industriel français est sous-traitant
Attestations internationales de sécurité Connaître l'habilitation d'une personne morale, ou entamer une procédure d'habilitation en sa faveur Connaître l'habilitation d'une personne physique, ou entamer une procédure d'habilitation en sa faveur Complément d'enquête de sécurité pour un individu ayant résidé à l'étranger ou pour un ressortissant étranger dont on souhaiterait l'équivalent d'un contrôle élémentaire Prouver l'habilitation d'un individu pour l'accomplissement d'une mission à l'étranger	Formulaire Facility Security Clearance Information Sheet (FSCIS) Personnel Security Clearance Information Sheet (PSCIS) Personnel Security Clearance Assurance Request (PSCAR) Certificat de sécurité ou PSCIS ou RFV (selon le contexte et les règlements applicables)
Acheminement d'informations et supports classifiés par porteur	Certificat de courrier
Acheminement d'informations et supports classifiés par fret	Plan de transport
Visite à l'étranger Avec échange d'informations et supports classifiés à partir nominalement du niveau <i>Secret</i> ou du niveau <i>Diffusion Restreinte</i> si les accords ou les règles de sécurité du projet mené le prévoient ou si la réglementation du pays hôte l'exige pour accéder à certains sites sensibles	Formulaire de Demande de visite – Request For Visit (RFV)
Visite depuis l'étranger Avec échange d'informations et supports classifiés à partir du niveau <i>Secret</i>	Formulaire de Demande de visite – Request For Visit (RFV)

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.2****3. Démarche à entreprendre par l'officier de sécurité**

Préalablement à l'échange d'informations et supports classifiés avec l'étranger, il est nécessaire de vérifier les éléments suivants :

- existence d'un cadre juridique avec le pays dont relève son interlocuteur ;
- connaissance des règles prévues dans cet accord par les participants concernés par l'échange d'informations ;
- s'il s'agit d'un industriel étranger, l'habilitation de la société et la détention par la société des aptitude physique et informatique pour détenir et traiter les informations et supports classifiés qui lui seront confiés ;
- habilitation de l'interlocuteur (selon le contexte et les règlements de sécurité qui couvrent l'échange) ;
- existence entre les deux pays d'une liaison électronique sécurisée et homologuée par les autorités nationales de sécurité et les autorités de sécurité respectives si l'information est transmise par voie numérique ;
- autorisation de la transmission de l'information classifiée par le pays d'origine de l'information ;
- couverture de l'échange par une licence d'exportation (s'adresser à DGA/DI ou EMA/MA).

Les informations relatives aux correspondants étrangers et à leurs autorités d'emploi, en particulier lorsqu'il s'agit de contractants étrangers, sont obtenues par les autorités nationales de sécurité/autorités de sécurité déléguées en utilisant les formulaires internationaux de demande d'informations reconnus par les parties concernées conformément aux stipulations de l'accord de sécurité applicable à l'échange considéré.

L'accès des correspondants étrangers est limité au strict besoin d'en connaître et dans la mesure où ils sont affectés dans un emploi nécessitant l'accès à des informations et supports classifiés, ils sont habilités aux niveaux appropriés. Les conditions générales d'habilitation des ressortissants étrangers sont fixées dans la fiche 3.8 de la présente instruction.

4. Marquages

Ce point est précisé dans l'annexe 37 de l'IGI 1300.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.3****CAS SPÉCIFIQUE DES CONTRATS INTERNATIONAUX : PLAN CONTRACTUEL DE SÉCURITÉ INTERNATIONAL (PCSI)****Référence :**

- IGI 1300 – 4.4.2.3.a

Points clés

- Un plan contractuel de sécurité international est établi pour définir les mesures de sécurité applicables et servir de vecteur de transmission des informations et supports classifiés dans le cadre d'un accord intergouvernemental, partenariat, convention ou contrat impliquant l'accès à des informations et supports classifiés entre entités de nationalités différentes. Il est mis en place avant tout échange d'informations et supports classifiés et couvre donc les phases amont telles que les phases précontractuelles.
- Dans le cadre d'un contrat ou d'une phase précontractuelle, le plan contractuel de sécurité international constitue une annexe qui lie les partenaires.
- Les accords de sécurité prévoient la rédaction d'un plan contractuel de sécurité international (ou d'un ensemble de clauses équivalentes) pour tout projet, contrat classifié²⁵³ qui implique un échange d'informations et supports classifiés.

Un plan contractuel de sécurité international (PCSI)²⁵⁴ est établi pour définir les mesures de sécurité à appliquer dans le cadre d'un accord intergouvernemental, d'un partenariat, d'une convention ou d'un contrat impliquant l'échange d'informations et supports classifiés entre une personne morale de droit public ou privé et des personnes morales publiques ou privées de droit étranger. Dans la pratique, les informations de niveau *Diffusion Restreinte* qui sont également transmises ou échangées sont incluses dans le plan contractuel de sécurité international couvrant les échanges d'informations et supports classifiés.

En cas d'accord de sécurité, si l'accord le spécifie ou ne mentionne aucune disposition en fonction du contexte, de la sensibilité du projet, de la nature ou du volume des informations et supports classifiés échangés, il revient à la personne morale de droit français émettrice de saisir son autorité nationale de sécurité ou autorité de sécurité déléguée pour définir la conduite à tenir. Le plan contractuel de sécurité international est, en général, élaboré par l'organisme émetteur dans le cadre d'une phase de négociation précontractuelle, d'un contrat, ou d'une opération de coopération internationale. Il précise aux partenaires français et étrangers, étatiques ou industriels les exigences à prendre en compte pour assurer la protection des informations et supports classifiés échangés.

Dès le stade de demande de délivrance de licence de transfert ou d'exportation, l'industriel ou l'État concerné prépare le plus en amont possible, avec l'appui du service

²⁵³ Désigné par le terme « *classified contract* » dans les textes internationaux.

²⁵⁴ L'appellation internationale est SAL (*Security Aspect Letter*).

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.3**

du ministère de la défense concerné par le matériel exporté, la rédaction du plan contractuel de sécurité international.

Pour les contrats (y compris ceux en sous-traitance), il s'applique essentiellement aux types suivants :

- ceux passés par une autorité contractante française (étatique ou privée) avec un industriel ou titulaire étranger ;
- les contrats « export » conclus par un industriel français ou l'État français avec un État étranger ou avec un industriel étranger.

Lorsque la partie française est à l'origine du plan contractuel de sécurité international

Ce dernier permet d'assurer quatre fonctions :

- constituer la partie d'un contrat contenant les éléments relatifs à la sécurité, dont la référence au support juridique de protection des informations et supports classifiés (l'accord de sécurité) ;
- permettre le contrôle de la cohérence des informations transmises avec les termes de la licence d'exportation ;
- lister les informations et supports classifiés à échanger avec l'étranger et leur niveau de classification et de protection ou ceux à recevoir de l'étranger ;
- informer les autorités nationales de sécurité et autorité de sécurité déléguées étrangères sur l'envoi d'informations et supports classifiés français à des entités de leur pays et les responsabiliser sur le fait qu'elles doivent s'assurer, dans leur domaine de responsabilité, du respect des dispositions de protection des informations et supports classifiés conformément aux accords de sécurité signés.

Le plan contractuel de sécurité international est validé par l'autorité de sécurité déléguée avant recueil par la partie émettrice de la signature de la partie destinataire. Il est signé par les parties émettrices et destinataires. La partie française adresse alors une copie à l'autorité de sécurité déléguée.

Il comprend obligatoirement :

- un guide de classification de sécurité (*Security Classification Guide*) s'inspirant du guide de classification de l'instruction de sécurité programme lorsqu'elle existe ;
- la référence aux accords applicables ;
- la référence de la licence d'exportation ;
- les coordonnées des autorités de sécurité étrangères ;
- les coordonnées des destinataires de l'information ;
- les lieux d'exécution des travaux classifiés ;
- une clause contraignante pour que ses dispositions soient également appliquées aux sous-traitants du destinataire étranger.

Outre ces éléments, il répond aux exigences mentionnées en annexe 28 de l'IGI 1300. Celles-ci peuvent être adaptées par l'autorité publique contractante en liaison avec le titulaire sans pouvoir leur être contraires.

Une copie du plan contractuel de sécurité international signé est adressée pour information à :

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.3**

- l'autorité nationale de sécurité française (SGDSN) et l'autorité nationale de sécurité ou autorité de sécurité déléguée étrangère, pour surveillance du contrat selon les stipulations de l'accord de sécurité ;
- la DRSD, pour information et lien éventuel avec l'opération protégée mère dont il peut découler.

Le formulaire de plan contractuel de sécurité international est disponible sur le site internet Armement²⁵⁵.

Lorsque la partie étrangère est à l'origine du plan contractuel de sécurité international

Le représentant de la partie française (étatique ou industriel) s'assure que les informations obligatoires prévues dans un plan contractuel de sécurité international (voir paragraphes précédents) sont présentes dans le document proposé par la partie étrangère et s'assure que celui-ci est validé par l'autorité de sécurité déléguée avant signature.

La partie française adresse alors une copie à l'autorité de sécurité déléguée. Une copie est adressée pour information à l'autorité nationale de sécurité française et à la DRSD.

²⁵⁵ Cf. Site Armement (<https://armement.defense.gouv.fr/securite-et-habilitation>).

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.4****ÉCHANGES NUMÉRIQUES CLASSIFIÉS AVEC L'ÉTRANGER****Point clé**

Les mesures de protection des informations numériques classifiées ou protégées échangées avec l'étranger sont fixées par des accords internationaux ou des documents de sécurité les déclinant et assurent un niveau de protection équivalent au niveau national.

En sa qualité d'autorité nationale de sécurité, le SGDSN prescrit, coordonne et contrôle l'application des mesures propres à assurer la protection du secret dans les relations entre la France et les États étrangers ou les organisations internationales. A cet effet, il négocie les accords généraux de sécurité qui permettent d'échanger des informations et supports classifiés (cf. fiche 9.1). Ces accords précisent les modalités de transmission électronique d'informations classifiées avec un partenaire étranger. L'autorité nationale de sécurité peut déléguer cette compétence à une autorité de sécurité déléguée (cf. fiche 9.1).

Lorsque des informations et supports classifiés ou protégés *Diffusion Restreinte* français sont transmis dans des systèmes d'information relevant de la responsabilité d'États étrangers ou d'organisations internationales, des mesures de protection sont fixées par des accords ou des règlements de sécurité avec ces partenaires, qui assurent à ces informations un niveau de protection au moins équivalent à celui prévu par la réglementation française.

La protection des systèmes d'information traitant d'informations et supports classifiés ou protégés au niveau équivalent *Diffusion Restreinte* confiés à la France par des États étrangers ou par des organisations internationales est assurée conformément aux accords et aux règlements de sécurité établis avec ces partenaires. Ces accords et règlements font, le cas échéant, l'objet d'instructions complémentaires pour l'application de ces mesures en France.

Lorsque des systèmes d'information traitant des informations classifiées ou protégées au niveau *Diffusion Restreinte* sont utilisés en commun avec des systèmes de partenaires étrangers ou internationaux, ces systèmes font l'objet d'une homologation commune. Une telle homologation ne peut être effectuée que s'il existe un accord de sécurité. Les représentants des autorités d'emploi, de l'autorité de sécurité déléguée (ASD – cf. fiche 9.1), et, le cas échéant des autorités contractantes de référence sont conviés au comité d'homologation. La protection des informations hébergées sur de tels systèmes est d'un niveau au moins équivalent à celui prévu dans la présente instruction, au titre 6.

Lorsque des méthodes cryptographiques doivent être appliquées pour assurer la protection de la confidentialité, de l'intégrité et de la disponibilité de tels systèmes d'information, ces méthodes ou les produits associés sont expressément approuvés pour chaque cas précis par l'ANSSI.

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.5****MISSIONS ET SEJOURS À L'ÉTRANGER****Référence :**

- Circulaire n° 11400/ARM/SGA/DRH-MD/SR-RH/SDFM/FM5 relative aux conditions dans lesquelles les militaires peuvent franchir les limites du territoire national au titre d'une permission ou d'un congé

Points clés**Missions et déplacements professionnels avec détention ou consultation d'informations et supports classifiés :**

- Les demandes de visite à l'étranger impliquant des supports classifiés sont adressées par le chef d'entité à l'autorité de sécurité compétente (DGA au titre de son rôle d'Autorité de Sécurité Déléguée, États-majors pour les autres cas), qui les fait suivre à l'ambassade de France du pays d'accueil pour transmission à l'autorité nationale de sécurité ou l'autorité de sécurité déléguée étrangère.
- L'autorité de sécurité compétente atteste du niveau d'habilitation du missionnaire.

Séjours :

- Les permissions du personnel militaire à l'étranger font l'objet de mesures particulières, notamment pour les pays de certaines catégories.
- Lorsque les circonstances l'exigent, l'autorité compétente peut restreindre l'exercice de la liberté de circulation pour le personnel militaire.
- Le personnel civil relevant du ministère de la défense ou des entités contractantes n'est pas assujéti à ces deux dernières obligations mais informe son officier de sécurité, qui le renseignera sur les bonnes pratiques à adopter.

Dans tous les cas :

- En cas d'incident durant une mission ou un séjour, l'officier de sécurité fait rédiger par l'intéressé un compte-rendu à destination du service enquêteur.

1. Missions à l'étranger**a. Demandes de visite impliquant des supports classifiés**

Les demandes de visites impliquant des supports classifiés sont prévues dans les accords de sécurité. Elles se réalisent selon leurs modalités.

Hors de ce cadre et mis à part certains cas particuliers (pour certains programmes, ou visites vers des pays de l'EDIR/FA), les demandes de visites pour l'étranger de personnel (français ou étranger) employé par une administration ou une personne morale française impliquant des supports classifiés sont adressées par l'autorité de sécurité déléguée ou l'autorité de sécurité française compétente à l'ambassade de France dans le pays d'accueil (mission de défense). L'ambassade fait suivre la demande à l'autorité nationale de sécurité ou l'autorité de sécurité déléguée du pays d'accueil. Elle utilise le formulaire prévu soit le règlement international lorsqu'il existe, soit dans les documents

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.5**

du projet (instruction de sécurité programme fixant les règles de sécurité) soit celui du GMSI²⁵⁶.

La demande de visite est visée par l'autorité de sécurité française compétente afin d'attester du niveau d'habilitation du personnel candidat à la visite.

Pour le ministère, les autorités compétentes pour viser ces demandes de visites sont les autorités de sécurité déléguée dans leur domaine de compétence, en particulier la DGA, en tant qu'autorité de sécurité déléguée dans le domaine tel que spécifié dans la note de délégation du SGDSN concernant l'industrie de défense.

Ces dernières peuvent déléguer leur signature à tout chef de formation militaire ou direction/service subordonné nominativement désigné. Elles lui précisent par écrit les consignes à appliquer.

En l'absence de modalités spécifiques contraires (par exemple, définies dans une instruction de sécurité programme), les demandes de visites de ressortissants étrangers salariés formulées par des établissements français de droit privé (industriels de défense) sont traitées comme celles des ressortissants français du même établissement et également adressées à la même autorité française compétente (DGA/SSDI dans son domaine de compétence) qui fait suivre les demandes selon la procédure précitée. À défaut d'imprimé imposé par le cadre de coopération (AGS, ISP, etc.), le formulaire standard GMSI peut être utilisé.

Cas particulier pour les visites au sein des entités de l'OTAN : l'accès aux entités fait l'objet de consignes, régulièrement mises à jour, diffusées *via* les sous-réseaux *COSMIC*. Les visiteurs doivent être en possession de leur certificat de sécurité OTAN pendant la durée de leur visite.

Cas particulier de certains programmes, ou visites vers des pays de l'EDIR/FA : ce type de visite est traité directement d'officier de sécurité à officier de sécurité, lesquels sont chargés de certifier l'habilitation du visiteur auprès de l'établissement visité.

b. Sensibilisation des Français en mission à l'étranger

Afin de limiter les risques, le missionnaire se conforme aux conseils pratiques figurant dans la fiche 2.8 de la présente instruction.

La règle essentielle à suivre en cas d'incident est de rendre compte immédiatement à l'ambassade ou au consulat le plus proche. Il est donc indispensable de posséder les coordonnées des points de contact diplomatiques locaux à alerter en cas de problème. Il lui importe de faire preuve de maîtrise de soi en toute circonstance : réagir avec trop de nervosité devant une provocation complique l'intervention des autorités consulaires ou diplomatiques.

²⁵⁶ GMSI ou groupe multinational de sécurité industrielle (en anglais : *MIWSG*) est un groupe informel qui établit des documents de sécurité dont un document sur les visites internationales. Ce document s'appelle RFV « Request For Visit ».

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.5****2. Permissions et séjours à l'étranger****a. Personnel militaire**

La circulaire de référence classe les pays en différentes catégories : la catégorie 10, pour laquelle les militaires peuvent librement circuler et la catégorie 20 qui se subdivise en :

- catégorie 21 : pays pour lesquels l'autorisation de s'y rendre relève de la décision du ministre après avis du service localement compétent de la DRSD ;
- catégorie 22 : pays pour lesquels l'autorisation de s'y rendre relève de la décision du commandant de formation administrative après avis du service localement compétent de la DRSD ;
- catégorie 23 : pays pour lesquels l'autorisation de s'y rendre relève de la décision du commandant de formation administrative.

Pour les catégories 21, 22 et 23, le demandeur complète le formulaire SOPHIA, qui peut être téléchargé sur le site Intradef de la DRSD :

- pour la catégorie 21, l'autorité d'emploi demande par SOPHIA l'avis du service localement compétent de la DRSD, qui dispose de deux semaines pour émettre un avis après avoir, selon son appréciation, procédé à une sensibilisation individuelle et adresse la demande au cabinet du ministre pour décision au plus tard trois semaines avant le départ en permissions du militaire. En cas de procédure d'urgence (cas d'événement familial important), le commandant de formation administrative peut adresser directement au cabinet du ministre une demande d'autorisation de permission pour un pays de catégorie 21 ;
- pour la catégorie 22, l'autorité d'emploi demande par SOPHIA l'avis du service localement compétent de la DRSD. Celle-ci dispose de deux semaines pour émettre un avis après avoir vérifié que l'intéressé a joint le formulaire daté et signé attestant qu'il a pris connaissance de la fiche de sensibilisation et de conseils en ligne sur le site DRSD de l'Intradef. Le service peut exceptionnellement procéder à une sensibilisation. À défaut de réponse de la DRSD dans un délai de deux semaines à compter de la prise en compte de la demande dans l'application SOPHIA, le commandant de formation administrative peut signer le titre de permission. Il adresse alors une copie du titre de permission à la DRSD ;
- pour la catégorie 23, le commandant de formation administrative donne son autorisation et signe le titre de permission sans être tenu de solliciter l'avis de la DRSD.

Lorsque les circonstances l'exigent, l'autorité compétente peut restreindre davantage l'exercice de la liberté de circulation pour le personnel militaire.

En cas d'incident durant le séjour, le personnel militaire rédigera à son retour un compte-rendu détaillé à l'attention de son officier de sécurité (en annexe 4 de la circulaire de référence) qui le transmettra au correspondant DRSD.

b. Personnel civil du ministère de la défense et des personnes morales liées par contrats ou convention

Le personnel civil du ministère de la défense et des personnes morales contractantes est soumis aux obligations de signalement énoncées précédemment. Le personnel détenteur d'informations sensibles, *Diffusion Restreinte* ou habilité se rapproche alors de son officier de sécurité pour se renseigner sur les zones à risque ou les mesures à

TITRE 9 : PROTECTION DU SECRET DANS LES RELATIONS INTERNATIONALES**9.5**

adopter lors d'un déplacement ou un séjour à l'étranger. Ce dernier pourra alors utilement se rapprocher de la DRSD si le déplacement concerne un pays des catégories 21 à 23.

Il est également recommandé au personnel civil de consulter l'onglet « conseils aux voyageurs » sur le site du Ministère de l'Europe et des Affaires étrangères et de s'enregistrer sur la base Ariane lors de son déplacement.

Les incidents survenus durant le séjour d'un civil doivent être signalés à l'officier de sécurité par l'intéressé.

Tous les échanges relatifs aux demandes d'avis et aux comptes rendus d'incident entre la formation administrative et le poste RSD compétent se font, sauf urgence avérée, par voie électronique Intradef ou Internet sécurisé par Acid.

3. Rôle de l'officier de sécurité

L'officier de sécurité doit sensibiliser le personnel de son organisme sur les démarches à suivre en cas de mission ou séjour à l'étranger.

Pour les militaires, l'officier de sécurité se tient informé des modifications pouvant intervenir dans la catégorisation des pays.

La mise en garde des personnes en missions à l'étranger dépend de la situation. Elle est complète et s'effectue dans la mesure du possible sous la forme d'un stage d'information ou de sensibilisation, pour une première mission de type donné. Elle peut être plus rapide pour des missions de routine telle que la participation périodique à des réunions de travail faisant suite à un accord. La DRSD peut être sollicitée pour apporter son concours en matière de prévention.

En cas de sensibilisation avant départ ou d'entretien au retour, l'officier de sécurité facilite le contact entre l'intéressé et son correspondant DRSD. Selon les consignes données par l'autorité d'emploi du missionnaire, un compte-rendu peut être établi à l'issue de la mission, et systématiquement, en cas d'incident pendant la mission. Les informations recueillies sont transmises à l'organisme DRSD compétent par l'officier de sécurité ou l'autorité d'emploi du missionnaire.

Lorsqu'un missionnaire convoie des informations et supports classifiés, il se munit auprès de son officier de sécurité d'un certificat de courrier validé par une autorité de sécurité compétente (voir §1.a.). Dans ce cas, la sensibilisation au départ de mission et un compte-rendu en fin de mission sont systématiques.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

INTRODUCTION : GÉNÉRALITÉS

Références :

- IGI 1300 – 2.3.1.1, annexe 3
- Code pénal, article 122-7

Points clés

- La protection du secret de la défense nationale concourt à la sécurité des opérations et à la performance opérationnelle à l'étranger.
- Cinq types de situations ont été retenus : 1/ les missions de défense à l'étranger (MDD), 2/ les forces pré-positionnées (FP), 3/ les postes permanents à l'étranger (PPE) insérés dans un état-major multinational, 4/ les PPE isolés ou semi-isolés, 5/ les opérations extérieures (OPEX), missions opérationnelles (MISSOPS) et exercices de préparation opérationnelle.
- Les compromissions à l'étranger peuvent avoir des conséquences graves et immédiates sur les intérêts de la France, la sécurité de la force déployée, sur sa crédibilité ainsi que sur le bon déroulement de la mission, particulièrement dans un environnement multinational ou en opération.
- L'IGI 1300 ne traitant ni de la spécificité de la protection du secret à l'étranger ni de celle des opérations, les mesures réglementaires doivent être adaptées en fonction du contexte opérationnel.
- Dans le cadre très spécifique des opérations, une directive technique particulière, précise le référentiel normatif en prenant en compte les exigences et contraintes opérationnelles. Elle reconnaît le recours à l'état de nécessité et la mise en œuvre de mesures compensatoires, voire dérogatoires à la réglementation.

1. Champ d'application

La protection du secret de la défense nationale concourt à la sécurité des opérations et à la performance opérationnelle à l'étranger.

Compte tenu de la diversité des situations et au regard des modalités particulières d'application du droit français, la typologie suivante a été retenue :

- Les missions de défense à l'étranger (MDD)

Les MDD sont des lieux dépendants des représentations diplomatiques françaises et en général situées au sein des ambassades. A ce titre, elles sont protégées par la convention de Vienne. Les locaux des MDD font partie des zones protégées d'une représentation diplomatique, aux termes des arrêtés du ministre des Affaires étrangères. Le cadre légal et réglementaire français s'y applique.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

- Les forces pré-positionnées (FP)

Les FP sont installées au sein d'une emprise dont la sécurité est assurée par le détachement des forces françaises déployées sur place. Le cadre juridique est défini par un accord signé avec la nation hôte.

- Les postes permanents à l'étranger (PPE) insérés dans un état-major multinational

Ces PPE sont installés au sein d'une emprise dont la sécurité est assurée par une organisation internationale ou les forces de sécurité de la nation hôte. Le cadre juridique est défini par un accord signé avec cette dernière. La protection physique des locaux français relève à la fois des règles françaises et de celles de la nation hôte.

- Les PPE isolés ou semi-isolés : le cas des officiers de liaison ou officiers d'échange.

Les PPE isolés ou semi-isolés sont insérés au sein de la nation hôte. La sécurité est sous l'entière responsabilité de celle-ci.

- Les opérations extérieures (OPEX), missions opérationnelles (MISSOPS) et exercices de préparation opérationnelle à l'étranger.

Les forces sont déployées au sein d'emprises ou sur des sites dont la sécurité est de leur responsabilité²⁵⁷. Le cadre juridique est défini par les règles d'engagement ou par un accord signé avec la nation hôte.

2. Principes

Une attention particulière doit être portée à la sécurité des informations et supports classifiés, ainsi qu'aux systèmes numériques associés lors d'une mission ou un déploiement à l'étranger. Quel que soit le contexte, l'absence de maîtrise de son environnement, les situations de crise ou le travail dans un cadre multinational peuvent conduire à des négligences, voire des ingérences, de nature à compromettre le secret de la défense nationale.

En particulier, le marquage des informations et supports classifiés, de ceux de niveau *Diffusion Restreinte* et sensibles doit intégrer une éventuelle communauté d'échange (« communicable à... ») ou une restriction de diffusion (*Spécial France* par exemple). Le besoin d'en connaître doit être respecté avec la plus grande rigueur, en toutes circonstances (accès aux supports, aux systèmes numériques, aux locaux, lors de réunions, etc.).

Les compromissions en opération ou en mission à l'étranger peuvent ainsi avoir des conséquences graves et immédiates sur la sécurité de la force déployée, sur sa crédibilité ainsi que sur le bon déroulement de la mission. Dans ce cadre et afin de limiter les risques et les effets d'une compromission, des dispositions préventives et limitatives spécifiques doivent être prises en considération.

²⁵⁷ Dans le cadre des exercices de préparation opérationnelle à l'étranger, la sécurité du personnel et des moyens français engagés peut relever des forces de sécurité du pays hôte, en particulier pour les bases aériennes et les ports, voire des sites de stationnement ou d'entraînement terrestres.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

L'IGI 1300 ne traitant ni de la spécificité de la protection du secret à l'étranger ni de celle des opérations, les mesures réglementaires (notamment les dispositions relatives à la protection physique décrites dans le titre 5 de la présente instruction) peuvent être adaptées en fonction du cadre juridique, du contexte opérationnel et des capacités matérielles accessibles dans le pays considéré.

3. Adaptation des mesures de protection

À l'étranger et plus particulièrement en opération, les mesures de protection du secret doivent être adaptées au contexte. Elles dépendent du cadre juridique existant et sont adaptées à la menace identifiée. Elles sont réalisées avec les moyens disponibles et autorisés par l'autorité responsable. En opération, les premières mesures de protection sont assurées par le dispositif de protection de la force, en particulier lors de la phase de projection ou d'entrée en premier sur le théâtre. Dans la durée, les mesures de protection physiques et logiques doivent se rapprocher autant que possible des mesures fixées par la présente instruction.

Toute adaptation de ces règles doit viser une compensation systématique des mesures ne pouvant être localement appliquées, par des moyens matériels, organisationnels et humain.

4. Directive technique particulière pour les opérations (DTPO)

Dans le cadre des opérations, une directive technique particulière précise le référentiel normatif afin que soient prises en compte les exigences et contraintes opérationnelles. Elle reconnaît le recours à l'état de nécessité (article 122-7 du code pénal) autorisant la mise en œuvre de mesures dérogatoires nécessaires à la sauvegarde des personnes ou des biens et proportionnées à un danger actuel ou imminent.

Cette directive prend en compte les conditions de l'engagement opérationnel, fait de pression, d'urgence et de performance. Elle s'applique aussi bien pour les opérations à l'étranger que pour les opérations sur le territoire national.

Ainsi, dans les cas où il est manifestement impossible de mobiliser des mesures compensatoires, la DTPO prévoit de pouvoir déroger à l'application des règles, procédures et dispositifs requis par la présente instruction pour la protection du secret et la sécurité des systèmes numériques classifiés. Cette décision de déroger doit prendre en compte les résultats d'une analyse de la menace, les capacités de l'adversaire à s'emparer, capter ou intercepter des données classifiées ou sensibles issues des systèmes numériques, afin de ne pas exposer la force à des vulnérabilités.

Dès que les conditions matérielles, techniques et tactiques le permettent, la chaîne de protection du secret et la chaîne de sécurité numérique doivent proposer au commandement de la force des mesures de sécurité des informations, supports et systèmes classifiés afin de se rapprocher autant que possible des mesures de protection fixées par la présente instruction.

**TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN
OPÉRATION****10.1****STRUCTURES ET INSTRUMENTS DE PILOTAGE ET DE MISE EN
OEUVRE****Référence :**

- IGI 1300 – 2

Points clés

- Toute personne habilitée est personnellement et pénalement responsable des modalités de conservation des informations classifiées qu'elle détient ou de leur divulgation à des tiers non qualifiés, à l'étranger comme en France
- Selon le type de déploiement, le commandement rédige une politique de protection du secret et met en place une chaîne de sécurité sous la responsabilité d'un officier de sécurité.
- La DRSD assure les mêmes missions au profit des unités à l'étranger qu'en France. Selon le besoin et la mission, elle peut déployer des postes ou des détachements de contre-ingérence pour les opérations ou réaliser sa mission à partir du territoire national.

1. La chaîne de responsabilité

La responsabilité de toute personne habilitée peut être engagée en cas de divulgation d'informations classifiées à des tiers non qualifiés ou de non-respect des modalités de conservation telles que décrites dans la présente instruction, en dehors du territoire national. Cette responsabilité couvre les informations strictement nationales et les informations étrangères confiées à la France ou partagées dans le cadre d'une coalition, dans un contexte UE ou OTAN ou en vertu d'un accord bilatéral.

a. Cas des missions de défense, des forces de présence et des postes permanents à l'étranger insérés en état-major multinational

Le commandant de la force ou le responsable d'organisme (mission de défense, représentation militaire française, etc.) rédige une politique de protection du secret qui s'applique à l'ensemble des personnes placées sous sa responsabilité. Il désigne un officier de sécurité et, le cas échéant, un officier de sécurité des systèmes d'information. Si l'effectif considéré est trop restreint, il assume lui-même ces fonctions (cas d'un attaché de défense par exemple).

b. Cas des postes permanents à l'étranger isolés ou semi-isolés (officiers de liaison et officiers d'échange)

Le personnel isolé ou semi-isolé dépend directement de l'officier de sécurité de niveau 1 auquel il est rattaché.

c. Cas des opérations, missions et exercices de préparation opérationnelle à l'étranger

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.1

Le commandant de la force ou du contingent national désigne un officier de sécurité de théâtre, qui est subordonné fonctionnellement à l'officier de sécurité du CEMA.

Il définit une chaîne de protection du secret et dirige le bureau de protection du secret. Des officiers de sécurité sont également désignés dans chaque formation ou sur chaque site.

Le commandant de la force ou du contingent national peut également désigner une chaîne de sécurité numérique qui participe à la protection des ACSSI, informations et des données classifiées.

Les chaînes de protection du secret et de sécurité numérique bénéficient de l'appui et du conseil du détachement de contre-ingérence armé par la DRSD sur le théâtre.

2. La direction du renseignement et de la sécurité de la défense (DRSD)

La DRSD, service de renseignement de contre-ingérence et service enquêteur pour le ministre de la défense, assure la continuité de ses missions auprès des formations déployées à l'étranger, de façon permanente ou temporaire, en opération ou en exercice.

À cet effet, elle arme des détachements de contre-ingérence ou des postes permanents sur la plupart des théâtres ou pays de déploiement et composantes navales embarquées.

Le détachement ou poste de la DRSD exerce en particulier les fonctions suivantes :

- il participe au comité de renseignement de théâtre afin de délivrer une analyse de la menace contre la force ;
- il conseille le commandant de la force ou du contingent national en matière de contre-ingérence ;
- il participe à la sensibilisation du personnel aux mesures de sécurité, y compris de protection du secret et de sécurité numérique ;
- il réalise les inspections, audits et contrôles dont le périmètre est fixé par l'autorité commanditaire ;
- il réalise les premières investigations en cas de suspicion de compromission d'une information ou support classifié.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.2

MESURES APPLICABLES AUX PERSONNES PHYSIQUES

Référence :

- IGI 1300 – 3

Points clés

- Au même titre que sur le territoire national, l'accès à l'étranger aux informations et supports classifiés est subordonné à l'habilitation du personnel concerné et à son besoin d'en connaître. Le besoin est décrit sur un catalogue des emplois.
- Le personnel affecté à l'étranger est habilité selon la procédure décrite au titre 3.
- Le personnel déployé en opération ou en mission à l'étranger est habilité par l'autorité d'habilitation de son organisme d'affectation. Un certificat de sécurité lui est fourni pour la mission.
- Une enquête de sécurité même succincte est réalisée par le détachement de contre-ingérence pour le personnel local ou étranger, civil ou militaire.

Au même titre que sur le territoire national, l'accès aux informations et supports classifiés à l'étranger est subordonné à l'habilitation du personnel concerné et à son besoin d'en connaître.

1. Catalogue des emplois

Concernant les opérations, le tableau unique d'effectifs et matériels (TUEM) décrivant chaque emploi et l'habilitation associée, tient lieu de catalogue des emplois. Il doit être réalisé au juste besoin, en cohérence avec le niveau de classification des informations et des systèmes numériques déployés.

2. Habilitation du personnel

a. Personnel affecté à l'étranger

Le personnel affecté à l'étranger est habilité selon la procédure décrite au titre 3 de la présente instruction.

Les procédures de demande d'habilitation doivent être initiées le plus tôt possible pour que chaque personne affectée détienne, avant son départ, l'attestation d'habilitation correspondant au niveau d'habilitation exigé.

b. Personnel déployé en opération, en mission ou en exercice à l'étranger

Le personnel déployé en opération, en mission ou en exercice à l'étranger est habilité par l'autorité d'habilitation de son organisme d'affectation. Un certificat de sécurité lui est fourni pour la durée de la mission.

Le responsable de l'organisme d'affectation doit ainsi vérifier le niveau d'habilitation requis pour le poste sur lequel est désignée chaque personne, en particulier dans un cadre multinational où une habilitation OTAN ou UE est requise.

En fonction de l'habilitation détenue au sein de son organisme d'affectation, une demande d'habilitation doit être effectuée en tenant compte des délais d'enquête.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.2

La décision d'habilitation temporaire est à privilégier pour le personnel détenant une habilitation au niveau *Secret* et devant être habilité au niveau *Très Secret* pour l'opération, la mission ou l'exercice.

Par ailleurs, le commandement transmet sur place à la DRSD, via l'officier de sécurité de sa formation, la liste du personnel désigné pour effectuer les vérifications de sécurité requises avant la projection.

3. Enquêtes administratives concernant le personnel étranger

a. Main d'œuvre locale

Une force, une composante ou un détachement français déployé à l'étranger peut recourir au service de personnel local (interprètes, personnel ayant des compétences intéressant la force déployée²⁵⁸, personnel d'entretien, etc.). Une investigation est réalisée par le détachement de contre-ingérence, armé par la DRSD, afin d'établir, dans la mesure du possible, si les personnes intéressées font l'objet de vulnérabilités. Un avis de sécurité est transmis à l'officier de sécurité du théâtre ou de l'organisme employeur, qui tient compte des conditions d'exécution des emplois proposés.

Une catégorisation des emplois et du personnel qui les occupe est établie en fonction du niveau de confidentialité et de sensibilité des informations auxquelles ce dernier peut avoir accès :

- Catégorie 1 : accès à des informations classifiées ou à des informations de niveau *Diffusion Restreinte* ou sensibles à caractère opérationnel ;
- Catégorie 2 : accès à des informations *Diffusion Restreinte* ou sensibles sans caractère opérationnel ;
- Catégorie 3 : accès à des informations non sensibles.

L'employeur décide d'accepter ou de refuser l'emploi d'une personne ou d'aménager contractuellement les conditions de son travail.

Toute personne morale de droit privé souhaitant passer un contrat ou une convention avec une force, une composante ou un détachement français déployé à l'étranger doit également faire l'objet préalablement d'une investigation conduite par le détachement de contre-ingérence armé par la DRSD. Elle porte, selon les informations que ce dernier pourra obtenir, sur les dirigeants, le capital, les activités et la réputation de cette personne morale.

²⁵⁸ Expert du BTP, architecte, etc.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.2

b. Militaires étrangers insérés dans les états-majors français

La présence de militaires étrangers insérés dans les états-majors nationaux est, le plus souvent, couverte par des accords multinationaux ou bilatéraux de sécurité qui fixent les règles applicables en matière de protection du secret. Si le besoin d'habiliter le militaire étranger est requis pour la mission, la demande doit respecter la procédure décrite dans les accords de sécurité et dans la fiche 3.8 de la présente instruction. En cas d'absence d'accord de cette nature, il ne peut être délivré d'habilitation.

Les militaires étrangers insérés dans les états-majors nationaux, même dûment habilités, ne peuvent prendre connaissance en aucune circonstance des documents portant la mention *Special France* .

**TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN
OPÉRATION****10.3****SÉCURITE DES LIEUX ABRITANT DES INFORMATIONS ET
SUPPORTS CLASSIFIÉS À L'ÉTRANGER ET EN OPÉRATION****Référence :**

IGI 1300 – 5

Points clés

- La protection juridique conférée par les dispositions du code pénal et du code de la défense relative aux différentes zones placées sous la responsabilité de l'autorité militaire (ZP et ZR en particulier) ne s'applique pas en dehors du territoire de la République.
- Le commandant de la force, composante ou détachement français définit les mesures de protection du personnel, du matériel et des informations, en fonction des contraintes liées à l'opération et de la nature des infrastructures disponibles. Ces règles doivent tendre vers l'application de la réglementation nationale, tout en s'inscrivant dans le respect du droit applicable sur le territoire de l'État hôte et du traité bilatéral ou de l'accord intergouvernemental applicable.
- Les mesures de protection adoptées doivent répondre à une analyse de risques effectuée pour chaque site de déploiement et répondre au principe de défense dans la profondeur.
- Il peut être défini des zones à accès contrôlé (ZAC) ou réservé (ZAR) dont l'objectif est de restreindre l'accès aux informations et supports classifiés par des mesures de protection adaptées.

La protection juridique conférée par les dispositions du code pénal et du code de la défense relative aux différentes zones placées sous la responsabilité de l'autorité militaire (zone militaire et zone protégée en particulier) ne s'applique pas en dehors du territoire national. En conséquence, les règles de protection prises localement doivent tendre vers l'application de la réglementation nationale, tout en s'inscrivant dans le respect du droit applicable sur le territoire de l'État hôte et du traité bilatéral ou de l'accord intergouvernemental applicable.

1. Les impératifs de protection : généralités

Le commandant de la force, composante ou détachement français définit les mesures de protection du personnel, du matériel et des informations, en fonction des contraintes liées à l'opération et de la nature des infrastructures disponibles. Ces mesures de protection doivent répondre à une analyse de risques réalisée pour chaque site de déploiement qui doit prendre en compte *a minima* :

- la protection physique des installations, du personnel et des matériels ;
- la protection des informations classifiées, de niveau *Diffusion Restreinte* et sensibles ;
- la protection des systèmes numériques ;
- des mesures d'évacuation d'urgence et de destruction.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.3

La conservation des informations et supports classifiés ainsi que l'accès aux systèmes numériques associés doivent répondre à une équation de sûreté adaptée au contexte opérationnel et aux ressources locales. Dans tous les cas, les mesures de protection doivent se rapprocher au plus près des mesures fixées dans la présente instruction.

Des zones spécifiques peuvent être créées : les zones à accès contrôlé (ZAC) et zones à accès réservé (ZAR).

2. Les mesures de protection physique

Il convient de protéger, par des mesures physiques appropriées, chaque emprise, zone, bâtiment, local, meuble, navire, aéronef ou véhicule, dans lequel sont conservés, traités ou manipulés, même temporairement, des informations et supports classifiés.

Les lieux abritant des informations et supports classifiés font l'objet d'un recensement annuel par l'officier de sécurité de niveau 1 dont ils dépendent, s'ils sont constitués d'infrastructures pérennes (forces pré-positionnées, missions de défense, états-majors, etc.).

Les lieux temporaires pour des exercices, missions à durée limitée ou opérations ne sont pas intégrés au recensement annuel. Le responsable de chaque site, l'officier de sécurité et le détachement local de la DRSD doivent cependant détenir une liste de ces lieux abritant temporaires dont le nombre doit être limité au juste besoin.

a. Niveaux de protection

Conformément au titre 5 de la présente instruction, plusieurs barrières doivent être mises en place en fonction du niveau de classification des informations à protéger. Elles constituent un dispositif retardant ou dissuadant l'intrusion, constitué de barrières successives selon le principe de défense dans la profondeur : protection périmétrique, bâtiment ou zone, local puis meuble éventuel.

Ce schéma de protection doit être respecté autant que possible de même que la conjugaison de mesures actives et passives : protection mécanique, mesures organisationnelles, systèmes de surveillance, de détection, d'alarme, moyens de levée de doute et d'intervention.

b. Les zones à accès contrôlé et zones à accès réservé

Un responsable de site peut définir une zone à accès contrôlé, pour restreindre et protéger l'accès à des lieux abritant du secret de la défense nationale ou une zone regroupant des lieux abritant. La création d'une telle zone peut nécessiter un accord préalable de l'État hôte.

Une zone à accès contrôlé doit répondre autant que possible aux caractéristiques d'une zone protégée sur le territoire national, en termes de protection périmétrique, de contrôle des accès, de détection intrusion, de capacité d'intervention dans la zone pour freiner une intrusion. Elle doit être délimitée et signalée de manière évidente pour empêcher l'accès à cette zone par inadvertance. Le responsable de site doit définir un régime de fonctionnement qui décrit à *minima* les conditions d'accès du personnel à

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.3

cette zone et les mesures de protection et d'intervention mises en œuvre. La création d'une zone à accès contrôlé est recommandée pour tous les centres ou salles opérations et pour tous les bureaux renseignement.

Une zone à accès réservé peut être décrite à l'intérieur d'une zone à accès contrôlé. Leur périmètre peut être confondu. La zone à accès réservé est destinée à abriter des informations et supports classifiés de niveau *Très Secret*.

Une zone à accès réservé doit répondre autant que possible aux caractéristiques d'une zone réservée sur le territoire national, en termes de protection périmétrique, de contrôle des accès, de détection d'intrusion, de capacité d'intervention dans la zone pour freiner une intrusion. Elle doit être délimitée et signalée de manière évidente pour empêcher un accès à cette zone par inadvertance. Elle est placée sous la responsabilité de l'officier de sécurité du site, qui doit définir un régime de fonctionnement. Ce dernier doit décrire *a minima* les conditions d'accès du personnel à cette zone et les mesures de protection et d'intervention mises en œuvre.

Une zone à accès réservé doit faire l'objet dès que possible d'un avis technique d'aptitude physique du service enquêteur, si cette zone se trouve au sein d'une infrastructure pérenne. Cette disposition ne s'applique pas aux opérations, missions à durée limitée ou exercices. Cependant, pour ces derniers cas, le conseil du détachement de contre-ingérence est à rechercher systématiquement.

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.4

SÉCURITÉ DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

Référence :

- IGI 1300 – 6

Points clés

- Les règles de traitement des informations et supports classifiés sont les mêmes en opération ou à l'étranger que sur le territoire national. Des mesures compensatoires ou dérogatoires peuvent néanmoins être prises en fonction de l'environnement et du contexte.
- La dématérialisation des informations classifiées doit être privilégiée afin d'en faciliter la gestion et la protection.

Les modalités de gestion des informations et supports classifiés décrites dans la présente instruction s'imposent sur le territoire national comme en opération ou à l'étranger. Seules les mesures d'acheminement et de conservation font exception. Des mesures d'évacuation et de destruction d'urgence sont impérativement définies et connues de chaque détenteur, y compris pour les sites isolés. Ces procédures sont définies dès l'arrivée sur le territoire.

Compte tenu des conditions de conservation et de transport, la dématérialisation des informations classifiées doit être privilégiée afin d'en faciliter la gestion et la protection.

Enfin, la gestion particulière des archives des opérations s'impose dès le déclenchement de l'opération. Des mentions spécifiques, ajoutées aux timbres de classification peuvent par ailleurs être créées pour chaque opération, mission ou exercice de préparation opérationnelle à l'étranger, en particulier dans un cadre multinational où l'information peut être partagée, afin de maîtriser la diffusion pertinente de l'information.

1. Durée de vie des classifications

Au cours d'une opération, de même qu'à la fin de celle-ci ou d'une mission ou exercice de préparation opérationnelle, le niveau de classification des informations et supports doit être réévalué régulièrement, afin de le maintenir au juste besoin.

Des informations peuvent être ainsi déclassifiées ou déclassées après une phase opérationnelle particulière tandis que certaines informations concernant les capacités techniques des armements ou systèmes d'observations, les sources ou techniques de renseignement par exemple, doivent rester classifiées pour de plus longues durées.

2. Mesures d'acheminement

Les modalités et les conditions d'acheminement des informations et supports classifiés à l'étranger dans le cadre d'une opération, d'une mission ou d'un exercice de préparation opérationnelle doivent être définies en intégrant l'analyse de risques, les

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.4

vulnérabilités propres aux conditions de transport et à la situation du site de déploiement dans le pays hôte.

À l'exception des missions de défense, les états-majors, directions et services peuvent demander au SGDSN la mise en place d'informations et supports classifiés de façon dérogatoire aux mesures décrites au titre 7 de la présente instruction. Le recours au certificat de courrier doit être privilégié, même s'il ne garantit aucune immunité juridique au convoyeur et au fret classifié qu'il accompagne.

L'utilisation de moyens de chiffrement des informations classifiées est à appliquer dès que possible (en particulier pour le personnel isolé ou les missions de faible effectif) et un accueil par le personnel de la mission de défense ou la représentation diplomatique française est à privilégier dans la mesure du possible.

3. Mesures de conservation

Les mesures de conservation doivent être précisées en fonction des capacités de stockage sécurisé disponibles dans le pays hôte et tendre à respecter au mieux les dispositions générales de conservation des informations et supports classifiés. Ainsi, des mesures compensatoires doivent être prises afin de pallier, à travers une garde permanente par exemple, l'absence de meuble ou de local sécurisé.

Le personnel en mission isolée (équipage d'aéronef etc.), détenteur d'informations ou supports classifiés s'adresse en priorité à la représentation française (mission de défense, ambassade ou consulat) pour lui confier, si nécessaire, la garde des documents ou supports. En cas d'impossibilité, il doit les conserver.

Dans ce cas, le personnel met en place une garde permanente ou utilise tout dispositif qu'il juge le plus proche des conditions réglementaires de conservation, comme un coffre de campagne.

En cas de suspicion de compromission, le commandement de la mission ou du détachement, la mission de défense et la DRSD doivent être informés dans les plus brefs délais.

**TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN
OPÉRATION****10.5****GESTION ET RÉPRESSION DES ATTEINTES AU SECRET DE LA
DÉFENSE NATIONALE****Référence**

- IGI 1300

Points clés :

- À l'étranger comme en opération, toute compromission peut avoir des répercussions dépassant l'intérêt propre des informations compromises.
- Des mesures préventives ou limitatives doivent systématiquement être prises.
- En cas de compromission, une enquête est systématiquement diligentée par la DRSD localement ou à partir du territoire national.
- En cas de suspicion de compromission, la responsabilité pénale personnelle de l'auteur étant engagée, ce dernier s'expose à des poursuites pénales.

À l'étranger comme en opération, toute compromission peut avoir des répercussions dépassant la valeur des informations compromises. Elle peut, en particulier, mettre en danger la vie de ressortissants ou militaires français et alliés ou nuire directement aux intérêts français.

1. Recommandations générales

La prévention des atteintes au secret de la défense nationale repose en particulier sur :

- la formation et l'instruction permanentes du personnel ;
- la sensibilisation par l'autorité organique avant le départ, adaptée au pays dans lequel a lieu la mission ;
- l'adoption de consignes adaptées à la situation du lieu de la mission ;
- la mise en place de séances de sensibilisation complémentaires au profit des nouveaux arrivants sur le territoire étranger ou le lieu de la mission ou de l'exercice ;
- le contrôle de l'application des directives jusqu'aux détenteurs d'informations ou supports classifiés ;
- la vigilance sur l'évolution de la situation (adaptation aux évolutions de la menace ou des conditions d'exécution de la mission, dérives dues aux effets de la routine, etc.) ;
- la discrétion professionnelle en toutes circonstances, en particulier à l'égard du personnel étranger (prestataires et employés locaux, officiers de liaison, etc.).

2. Dispositions pratiques vis à vis des compromissions en opération, en mission ou en exercice à l'étranger**a. Mesures préventives**

Les principaux facteurs de vulnérabilité du secret et de mise en cause de sa protection sont la routine, le rythme rapide des activités, la banalisation du recours à la

TITRE 10 : PROTECTION DU SECRET À L'ÉTRANGER ET EN OPÉRATION

10.5

classification et ses dérives, l'absence d'expert dédié à cette fonction ou le sentiment d'impunité.

L'émission, l'acheminement et la conservation d'informations et supports classifiés sont à limiter au strict nécessaire.

La facilité de stockage et de transfert des outils numériques implique une grande rigueur et une vigilance accrue pour éviter de conserver sur un support mobile des informations, parfois sensibles, sans lien avec la mission en cours.

Les moyens de communication ou d'information, qu'ils soient à usages privés ou professionnels, peuvent être restreints ou interdits selon les vulnérabilités qu'ils induisent.

Afin de limiter les risques, un inventaire régulier doit être effectué afin de vérifier la présence physique exhaustive des informations et supports classifiés. Cet inventaire est obligatoire lors des relèves de postes et doit être conduit de façon contradictoire.

b. Mesures limitatives

Le recours aux dispositifs de chiffrement, lorsqu'ils existent, est fortement recommandé en particulier sur les ordinateurs portables et supports amovibles hors des enceintes protégées.

Tout support ou élément mobile ayant contenu des informations classifiées conserve le besoin de protection réglementairement requis par la nature même de ces informations. En effet, les opérations d'effacement de données et de reformatage de leur support ne garantissent aucunement une inaccessibilité aux informations classifiées supprimées.

La sauvegarde régulière des supports numériques est obligatoire car elle contribue, en cas de compromission, à définir le préjudice généré.

c. Traitement des compromissions

En cas de suspicion de compromission, le détachement de contre-ingérence armé par la DRSD doit être immédiatement informé. Une première investigation doit permettre de s'assurer que les vulnérabilités sont circonscrites et de préciser les circonstances de la compromission.

Lorsque les investigations confirment la suspicion de compromission, la DRSD, après avoir informé le responsable de l'organisme concerné et l'officier de sécurité, transmet le dossier à la DGSJ ou à la gendarmerie prévôtale sur les théâtres d'opérations extérieures ou en zone de stationnement des forces françaises. Cette dernière procède à l'enquête judiciaire.

En cas de compromission avérée, la responsabilité pénale personnelle de l'auteur étant engagée, ce dernier s'expose à des poursuites pénales.

ANNEXES

ANNEXE 1

LISTE DES EMPLOIS SENSIBLES

Sont notamment à considérer comme occupant un emploi sensible le personnel :

- servant dans l'environnement immédiat des hautes autorités²⁵⁹ ;
- servant dans les forces nucléaires ;
- affecté à la manutention, le transport, la comptabilité de matériels ou de produits présentant un caractère dangereux (armement, munitions et explosifs, carburant, substances toxiques)²⁶⁰ ;
- affecté à la préparation, au traitement, au conditionnement et au stockage des expéditions de fret, biens et produits transportés par les aéronefs, bâtiments de surface et sous-marins, utilisés par le ministère de la défense ;
- affecté à la réparation ou l'entretien des matériels considérés comme majeurs par les états-majors, directions, services ministériels ;
- transportant des informations et supports classifiés de niveau *Secret* ou *Très Secret* sur le territoire national (au titre de la décision de sécurité convoyeur)²⁶¹ ;
- affecté à une mission d'accueil, filtrage ou gardiennage des emprises du ministère de la défense (hors personnel externalisé) ;
- le personnel gérant les données RH du personnel des organismes dont les identités sont protégées par la loi²⁶² ;
- les administrateurs de systèmes numériques de niveau *Diffusion Restreinte* ;
- le personnel manipulant des informations confidentielles spécifiques (Ressources humaines, santé, etc.) (cf. fiche 3.11).

Les appellations utilisées *supra* sont génériques. Chaque état-major, direction ou service (EMDS) ministériel les précisera selon ses spécificités et en liaison avec la DRSD.

Le formulaire de demande à utiliser sur SOPHIA pour les enquêtes administratives préalables à l'accès à un emploi sensible exercé dans un des lieux mentionnés à l'article R. 114-4 du code de la sécurité intérieure est le CES (comme *Contrôle Emploi Sensible*) sauf pour le transport d'informations et supports classifiés pour lequel il faut remplir un formulaire CNV (comme *CoNVoyeur*).

²⁵⁹ Conducteur ou personnel de la maison militaire, par exemple.

²⁶⁰ Concerne le personnel spécialisé armurier ou comptable munitions par exemple et non le militaire portant ou servant son arme.

²⁶¹ Selon la mission décrite à l'article 36 de l'IGI de référence. Le transport du *Très Secret* classification spéciale fait l'objet de dispositions particulières.

²⁶² Cf. arrêté du 7 avril 2011 relatif au respect de l'anonymat de certains fonctionnaires de police et militaires de la gendarmerie nationale, arrêté du 7 avril 2011 relatif au respect de l'anonymat de militaires et de personnels civils du ministère de la défense et arrêté du 20 octobre 2016 relatif à la préservation de l'anonymat des membres des unités des forces spéciales.

ANNEXE 2

DÉCISION D'HABILITATION (PERSONNEL CIVIL)*Une fois complété ce document porte la mention :***DIFFUSION RESTREINTE**

DECISION D'HABILITATION
aux informations ou aux supports classifiés
(En référence à l'IGI 1300)

Le

Par la présente décision,

Monsieur, Madame :

né (e) le : à

fonctions :

affectation :

est habilité(e) pour accéder aux informations ou supports classifiés jusqu'au JJ/MM/AA

jusqu'au niveau et y compris : Niveau de classification à indiquer ici

Cette décision porte la référence SOPHIA :

Signature de l'autorité d'habilitation

Ministère des Armées
Direction/ Sous-Direction
Adresse :
Courriel

ANNEXE 3

DÉCISION D'HABILITATION (PERSONNEL MILITAIRE)

Une fois complété ce document porte la mention :

**DIFFUSION RESTREINTE**

DECISION D'HABILITATION
aux informations ou aux supports classifiés
(En référence à l'IGI 1300)

Le

Par la présente décision,

Monsieur, Madame :

né (e) le : à

fonctions :

affectation :

est habilité(e) pour accéder aux informations ou supports classifiés jusqu'au JJ/MM/AA

jusqu'au niveau et y compris : Niveau de classification à indiquer ici

Cette décision porte la référence SOPHIA :

Signature de l'autorité d'habilitation

Ministère des Armées
Direction/ Sous-Direction
Adresse :
Courriel :

ANNEXE 4

ENGAGEMENT DE RESPONSABILITÉ

Une fois complété ce document porte la mention :



DIFFUSION RESTREINTE

rection ...

ENGAGEMENT DE RESPONSABILITÉ

Un exemplaire de ce document doit être produit et signé pour chaque niveau et nature d'habilitation d'un agent

VOLET 1

Je, soussigné(e) (Prénom, NOM)

Poste/Grade/Fonction :

Service employeur :

Déclare :

- avoir été informé(e) de la décision actuellement en vigueur en date du m'autorisant l'accès à des informations et supports classifiés au niveau :

☐ TRES SECRET FRANCE☐ SECRET UE☐ SECRET OTAN☐ SECRET FRANCE☐ CONFIDENTIEL UE☐ CONFIDENTIEL OTAN

- avoir pris connaissance de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, ainsi que des dispositions du code pénal citées en références de l'instruction ;
- être pleinement conscient(e) de mes responsabilités en ce qui concerne la protection des informations et supports classifiés ;
- être informé(e) des conséquences prévues par les dispositions législatives (articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9 du code pénal) et réglementaires, notamment pour le cas où, sciemment ou par négligence, je laisserais ces informations et supports classifiés parvenir à des personnes non qualifiées.

En conséquence, **je m'engage à ne pas divulguer**, même après la cessation de mes fonctions ou de ma mission, à des personnes non qualifiées les informations et supports classifiés dont j'aurais connaissance dans l'exercice de mes fonctions ou l'accomplissement de ma mission.

À

le

Nom et signature de l'officier de sécurité

Signature de l'intéressé(e)

VOLET 2

À compter de la date de cessation des fonctions ou de ma mission, pour lesquelles une décision d'habilitation à connaître d'informations et supports classifiés m'a été délivrée, **je m'engage à ne pas divulguer à des personnes non qualifiées** les informations et supports classifiés dont j'ai eu connaissance dans l'exercice de mes fonctions ou pendant l'accomplissement de ma mission et **à ne conserver par-devers moi aucun support classifié**.

Je reconnais être informé(e) des **conséquences** prévues par les dispositions législatives (articles 121-2, 411-1 à 411-11, 413-9 à 413-12 et 414-7 à 414-9 du code pénal) et réglementaires, notamment pour le cas où, sciemment ou par négligence, je porterais à la connaissance de personnes non qualifiées ces informations et supports classifiés.

À

le

Nom et signature de l'officier de sécurité

Signature de l'intéressé(e)

Ministère des Armées
Direction/ Sous-Direction
Adresse :
Courriel :

ANNEXE 5

DÉCISION DE REFUS D'HABILITATION (PERSONNEL CIVIL)

Une fois complété ce document porte la mention :



DIFFUSION RESTREINTE

DECISION DE REFUS D'HABILITATION
aux informations ou aux supports classifiés
(En référence à l'IGI 1300)

Le

Par la présente décision,

Monsieur, Madame :

né (e) le à

fonctions exercées :

affectation :

fait l'objet d'une décision de refus d'habilitation pour l'accès aux informations ou supports classifiés.

Cette décision porte la référence SOPHIA :

La présente décision peut faire l'objet d'un recours contentieux auprès du tribunal administratif territorialement compétent dans le délai de deux mois à compter de sa notification, conformément aux dispositions de l'article R.421-1 du code de justice administrative.

La présente décision est notifiée à l'intéressé(e) conformément à l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

Signature de l'autorité d'habilitation

Ministère des Armées
Direction/ Sous-Direction
Adresse :
Courriel :

ANNEXE 6

DÉCISION DE REFUS D'HABILITATION (PERSONNEL MILITAIRE)

Une fois complété ce document porte la mention :



DIFFUSION RESTREINTE

DÉCISION DE REFUS D'HABILITATION
aux informations ou aux supports classifiés
(En référence à l'IGI 1300)

Le

Par la présente décision,

Monsieur, Madame :

né (e) le à

fonctions exercées :

affectation :

fait l'objet d'une décision de refus d'habilitation pour l'accès aux informations ou supports classifiés.

Cette décision porte la référence SOPHIA :

Conformément aux dispositions des articles R.4125-1 et suivants du code de la défense, la présente décision peut faire l'objet d'un recours auprès de la commission des recours militaires (CRM), dans un délai de deux mois à compter de sa date de notification.

La saisine de la commission est un préalable obligatoire à l'exercice d'un recours contentieux devant la juridiction administrative compétente, qui peut être formé, conformément aux dispositions de l'article R.421-1 du code de la justice administrative, dans un délai de deux mois à compter de la notification de la décision prise sur le recours.

La présente décision est notifiée à l'intéressé(e) conformément à l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

Signature de l'autorité d'habilitation

Ministère des Armées
Direction/ Sous-Direction
Adresse :
Courriel :

ANNEXE 7

**RÉCEPISSÉ DE NOTIFICATION D'UNE DÉCISION DE REFUS
D'HABILITATION OU D'ABROGATION D'UNE DÉCISION
D'HABILITATION (PERSONNEL CIVIL)**

Je soussigné(e) :

Reconnais que l'officier de sécurité de²⁶³ :

M'a notifié et remis ce jour la décision²⁶⁴ :

Prise par²⁶⁵ :

En date du :

Portant refus de délivrance / abrogation²⁶⁶ de l'autorisation d'accéder aux informations et supports classifiés au(x) niveau(x) :

☐ TRES SECRET

☐ TRÈS SECRET UE /
EU TOP SECRET

☐ COSMIC TRÈS SECRET /
COSMIC TOP SECRET

☐ SECRET

☐ SECRET UE /
EU SECRET

☐ NATO SECRET /
NATO SECRET

☐ CONFIDENTIEL UE /
EU CONFIDENTIAL

☐ NATO CONFIDENTIEL /
NATO CONFIDENTIAL

La présente décision peut faire l'objet d'un recours contentieux auprès du tribunal administratif territorialement compétent dans le délai de deux mois à compter de sa notification, conformément aux dispositions de l'article R.421-1 du code de justice administrative.

À

Le

Signature de l'intéressé(e)

²⁶³ Organisme

²⁶⁴ Référence de la décision

²⁶⁵ Autorité d'habilitation ou autorité ayant reçu délégation à cet effet

²⁶⁶ Rayer la mention inutile

ANNEXE 8

**RÉCEPISSÉ DE NOTIFICATION D'UNE DÉCISION DE REFUS
D'HABILITATION OU D'ABROGATION D'UNE DÉCISION
D'HABILITATION (PERSONNEL MILITAIRE)**

Je soussigné(e) :

Reconnais que l'officier de sécurité de²⁶⁷ :

M'a notifié et remis ce jour la décision²⁶⁸ :

Prise par²⁶⁹ :

En date du :

Portant refus de délivrance / abrogation²⁷⁰ de l'autorisation d'accéder aux informations et supports classifiés au(x) niveau(x) :

☐ TRES SECRET

☐ TRÈS SECRET UE /
EU TOP SECRET

☐ COSMIC TRÈS SECRET /
COSMIC TOP SECRET

☐ SECRET

☐ SECRET UE /
EU SECRET

☐ NATO SECRET /
NATO SECRET

☐ CONFIDENTIEL UE /
EU CONFIDENTIAL

☐ NATO CONFIDENTIEL /
NATO CONFIDENTIAL

Conformément aux dispositions des articles R.4125-1 et suivants du code de la défense, la présente décision peut faire l'objet d'un recours auprès de la commission des recours des militaires (CRM), dans un délai de deux mois à compter de sa date de notification.

La saisine de la commission est un préalable obligatoire à l'exercice d'un recours contentieux devant la juridiction administrative compétente, qui peut être formé, conformément aux dispositions de l'article R.421-1 du code de justice administrative, dans un délai de deux mois à compter de la notification de la décision prise sur recours.

À

Le

Signature de l'intéressé(e)

²⁶⁷ Organisme

²⁶⁸ Référence de la décision

²⁶⁹ Autorité d'habilitation ou autorité ayant reçu délégation à cet effet

²⁷⁰ Rayer la mention inutile

ANNEXE 9

**DÉCISION D'ACCÈS AUX INFORMATIONS ET SUPPORTS
CLASSIFIÉS POUR L'HABILITATION D'UNE PERSONNE PHYSIQUE
DANS LE CADRE D'UN CONTRAT OU D'UNE CONVENTION AVEC
LE MINISTÈRE DE LA DÉFENSE**

Une fois complété ce document porte la mention :

**DIFFUSION RESTREINTE**

rection ...

**Service de la sécurité
de défense et des systèmes
d'information**

Lieu, le

Objet : Décision d'accès aux informations ou aux supports
classifiés.

Référence de la demande : Demande n°

P. jointe : Décision n°

Monsieur le Directeur,

J'ai l'honneur de vous adresser la décision d'accès à des informations classifiées concernant Monsieur, Madame.

Je vous demande de bien vouloir inviter l'intéressé(e) à signer - sauf s'il s'agit d'un renouvellement - le volet I de l'engagement de responsabilité.

Cette décision annule et remplace la décision citée en référence.

À la cessation de fonction ou de mission de l'intéressé(e), vous voudrez bien me retourner la décision d'accès le concernant accompagnée des volets 1 et 2 de l'engagement de responsabilité dûment datés et signés par l'intéressé(e).

[À ajouter si nécessaire] Je vous informe, en outre, que conformément à la réglementation (article 25 de l'IGI 1300), une mise en éveil ou une mise en garde de l'intéressé(e) est demandée.

Je vous prie d'agréer, Monsieur le Directeur, l'assurance de ma considération distinguée.

Signature de l'autorité d'habilitation

Monsieur le Directeur de

«société»
«adresse»
«code_postal» «ville»

ANNEXE 10

(pour l'officier de sécurité)

DÉCISION DE CRÉATION DE ZONE RESERVÉE



Nom de l'organisme, du service

Lieu, le
N° /XXX/XXX/NPDÉCISION N° XXX/DATE/ORGANISME/SERVICE/NP
PORTANT CRÉATION D'UNE ZONE RESERVÉE

Nom du responsable d'organisme, fonction,

- Vu le code pénal et notamment... ;
- Vu l'arrêté du 9 août 2021 approuvant l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale ;
- Vu l'arrêté du (date) portant création de la zone protégée de l'emprise dénommée (nom de l'emprise) ;
- Vu l'instruction ministérielle n° 900/ARM/CAB relative à la protection de l'information et des données ;
- Vu l'avis technique d'aptitude physique n° (réf. de l'avis) du (date).

DÉCIDE :

ARTICLE 1 : la pièce XX située au (n° étage) du bâtiment XXXX est érigée en zone réservée.

ARTICLE 2 : cette zone réservée est intégrée dans la zone protégée désignée par l'arrêté du (date de l'arrêté) susmentionné.

Fait à (lieu), le (date).

Nom du responsable d'organisme
Fonction
(Signature)DESTINATAIRES :

- Officier de sécurité de l'organisme
- Bureau de protection du secret de l'organisme

COPIE :

- OS de l'entité responsable du site

ANNEXE 11

**LISTE DES PIÈCES CONSTITUTIVES DU DOSSIER TECHNIQUE
D'APTITUDE PHYSIQUE D'UN ÉTABLISSEMENT POUR L'EXÉCUTION
D'UN CONTRAT IMPLIQUANT LA DÉTENTION D'INFORMATIONS
ET SUPPORTS CLASSIFIÉS**

Il y a lieu de constituer autant de dossiers différents qu'il y a de lieux distincts d'exécution des travaux protégés.

1. Documents à fournir par la personne morale afin d'obtenir l'aptitude physique de ses locaux (Renseignements sur le lieu d'exécution des travaux classifiés)

- Analyse de risques réalisée par l'établissement.
- Plan de masse de l'établissement.
- Organisation et moyens de protection et de gardiennage de l'établissement.
- Identification et description de la protection, actuelle et envisagée, du local ou des locaux où sont exécutés les travaux protégés. Ceci inclut la liste des organismes assurant l'installation et la maintenance des systèmes numériques de sûreté concourant à la protection du local.
- Dossier de sécurité (DSSI).
- Décision d'homologation du système numérique de sûreté.
- Liste des sous-traitants intervenant dans l'établissement, faisant ressortir les prestataires de services au titre d'un contrat avec accès d'un contrat sensible.

2. Document préparé par l'autorité contractante ou le contractant (Complément à la définition et à la justification du besoin d'en connaître)

Plan contractuel de sécurité ou projet de plan contractuel de sécurité.

ANNEXE 12

RECOMMANDATIONS POUR LA MISE EN ŒUVRE ET LE FONCTIONNEMENT D'UN POSTE (CENTRAL) DE SÉCURITÉ D'UNE PERSONNE MORALE SOUS CONTRAT OU CONVENTION AVEC LE MINISTÈRE DE LA DÉFENSE

Références :

- Code du travail articles L.4121-3-1, articles R.4228-1, 4228-10 et 4228-22
- Référentiel APSAD²⁷¹ R8 Surveillance des risques
- Référentiel APSAD R31 Télésurveillance

Cette fiche comprend un ensemble de recommandations, à destination des acteurs mettant en œuvre un poste de sécurité. Elle n'a pas de portée prescriptive.

Points clés

- Le poste central de sécurité (PCS) est de préférence placé au cœur du site et à proximité des lieux sensibles.
- L'infrastructure du PCS doit permettre de rechercher son inviolabilité et sa résilience.
- L'organisation du PCS permet aux agents de travailler dans des conditions optimales.
- Le PCS centralise les systèmes d'information de sûreté surveillés par des agents formés, de préférence expérimentés et régulièrement contrôlés lors d'exercices.

La protection physique des lieux participe à la protection du secret de la défense nationale. L'efficacité des dispositifs techniques de protection mis en place repose, notamment, sur la réactivité des acteurs de la sécurité privée²⁷² (ASP) en charge de leur surveillance permanente. La gestion et la supervision de ces systèmes sont confiées à la structure de sécurité afin d'en assurer la cohérence et une exploitation optimale.

En l'absence de disposition législative ou réglementaire sur le sujet, cette fiche vient présenter les standards recherchés lors de la conception et l'installation d'un PCS ainsi que dans son fonctionnement quotidien. **Elle ne traite pas de la protection contre le risque incendie.**

Véritable poste de commandement placé sous le contrôle de l'officier de sécurité d'établissement, le PCS applique les consignes définies par le responsable de l'organisme auquel il appartient et propres à chaque emprise et site. Ses missions sont les suivantes :

- surveiller l'ensemble de l'emprise, des locaux, installations et parties non bâties du site ;
- coordonner sur toute l'emprise les missions des ASP ;
- surveiller les consoles des systèmes de sûreté et maîtriser leur fonctionnement ;

²⁷¹ Assemblée Plénière des Sociétés d'Assurances Dommages.

²⁷² Tel que prévu par l'article R.631-4 du code de la sécurité intérieure, par opposition aux acteurs de la sécurité publique.

- déclencher les interventions/levées de doute qui s'imposent et suivre leur déroulement ;
- réaliser des rondes et autres missions liées à la sûreté/sécurité de l'emprise et en contrôler l'effectivité (rondes internes, externes, de fermeture, d'ouverture, pointées, etc.) ;
- s'assurer de la traçabilité de chaque événement et incident relatifs à la sûreté/sécurité et en rendre-compte à la structure de sécurité de l'emprise (journal de surveillance ou main courante papier ou informatisée) ;
- diffuser l'alarme et l'alerte aux forces d'intervention compétentes.

1. Positionnement du PCS

L'emplacement du PCS est étudié au regard de la typologie du site et des missions qui lui sont confiées. Il est conseillé d'établir le PCS à proximité des valeurs à protéger tout en assurant sa propre protection et discrétion. Idéalement, il est installé au cœur de l'emprise, loin des limites de propriété et des accès routiers.

2. Infrastructure du PCS

L'infrastructure du PCS lui assure sa propre protection, contre l'intrusion et contre l'agression. Le local est donc sécurisé sur sa périmétrie (notamment les ouvrants) et est en permanence fermé. Les accès y sont contrôlés et limités aux seules personnes autorisées, idéalement à l'aide d'un dispositif d'identification et d'authentification. En effet, le PCS conserve la mémoire des incidents/événements survenus, héberge des données personnelles (enregistrement vidéo) et conserve, en général, les clés du site ou leurs doubles. Il est séparé du poste d'accueil ou de filtrage des visiteurs tout en restant en liaison permanente avec ce poste.

Son fonctionnement est permanent (il dispose d'un secours en énergie). Une gestion en mode dégradé doit être prévue et éprouvée. Idéalement, la redondance des systèmes de sûreté en place est prévue, sur site ou déportée sur une autre emprise dans un PCS existant, afin d'assurer une permanence de la surveillance par les agents. Quel que soit le fonctionnement adopté, les alarmes doivent aboutir au PCS, à l'agent où qu'il se trouve sur le site ou à la personne morale tierce en charge du service de télésurveillance.

3. Organisation du PCS

L'organisation du PCS satisfait, dans de bonnes conditions matérielles de travail, à un fonctionnement en continu, les ASP étant présents en permanence pour assurer la continuité de la surveillance.

L'ergonomie de chaque poste de travail nécessite un examen particulier selon les missions de l'agent (utilisation de souris, clavier et autres outils bureautiques, rayonnements et fatigue visuelle, fauteuils, etc.). La prise en compte de cette ergonomie réduit les incidences sur la santé de l'agent et sur sa concentration dans l'exécution de ses fonctions.

Si l'agent travaille seul, il convient de prévoir un dispositif d'alarme pour travailleur isolé (DATI).

La régulation de la température et de l'aération est à prévoir. La luminosité s'adapte à un travail de jour comme de nuit, tout en garantissant la confidentialité des affichages. L'isolation phonique permet aux agents de pouvoir se concentrer sur leurs fonctions.

Des locaux de confort (salle de repos et de restauration) ainsi que des locaux d'hygiène (vestiaires, sanitaires, douches) sont mis à disposition du personnel présent.

4. Exploitation du PCS

Le PCS centralise, notamment, les consoles de suivi et de traitement des systèmes de sûreté (contrôle d'accès, détection d'intrusion et vidéosurveillance). Ces consoles sont surveillées en permanence par des ASP qui apportent les réponses adaptées aux remontées s'affichant sur les consoles. Pour ce faire, ils disposent des outils nécessaires pour remplir leurs fonctions : cahiers de consignes claires et régulièrement mises à jour (celles établies par leur employeur et celles établies par le responsable de l'emprise), documents ou plans nécessaires à l'exécution des missions, main courante, moyens de communication (avec la structure de sécurité, lors des rondes, etc.), outils de gestion des clés, etc.

Le PCS peut être commun à plusieurs sites. Dans ce cas, le personnel en charge de la surveillance doit pouvoir identifier immédiatement le site à l'origine de l'alarme.

Les agents sont en mesure d'intervenir rapidement sur les zones à protéger afin de répondre au mieux à l'équation de sûreté.

Ils sont en contact régulier avec la structure de sécurité de l'emprise, voir, le cas échéant, installés à proximité. Ils sont également en lien avec le représentant de leur employeur.

Les agents tenant le PCS ont suivi une formation adaptée, régulièrement mise à jour, et disposent d'une carte professionnelle (délivrée par le Conseil national des activités privées de sécurité). La mise en œuvre des consignes est contrôlée régulièrement par la structure de sécurité de l'emprise (à l'occasion d'exercices, tests d'intrusion, évaluation délai intervention, etc.).

ANNEXE 13

GUIDE LIÉ AUX CONDITIONS D’EMPLOI DES NIVEAUX DE CLASSIFICATION SECRET ET TRES SECRET

Préambule :

Chaque état-major, direction ou service doit décliner un guide de classification spécifique à son périmètre de compétence. Il est adressé au FSD.

Concernant les installations, moyens et activités de la dissuasion, il existe un guide de classification interministériel édité et mis à jour sous l’égide du SGDSN.

En fonction du sujet traité, la classification peut être assortie de la mention *Spécial France*.

- Chapitre 1
- Questions d’ordre général
- Chapitre 2
- Questions relatives aux opérations
- Chapitre 3
- Questions relatives au renseignement
- Chapitre 4
- Questions relatives à la protection
- Chapitre 5
- Questions relatives à la logistique et à la mobilisation
- Chapitre 6
- Questions relatives aux systèmes d’information, de communication et de guerre électronique
- Chapitre 7
- Questions concernant les matériels, les systèmes d’armes et les recherches ou études correspondantes

TRÈS SECRET	SECRET
1- <u>QUESTIONS D'ORDRE GÉNÉRAL</u>	
Certaines études dans les domaines militaires (stratégiques, opératifs, tactiques, opérationnels et techniques) touchant aux concepts d'emploi des forces en opérations réelles, dans le domaine nucléaire et dans le domaine de la guerre électronique.	Certaines études dans les domaines militaires (stratégiques, opératifs, tactiques, opérationnels et techniques) touchant aux concepts d'emploi des forces en opérations réelles.
Certaines études nationales ayant trait à la conception, à la sûreté, à l'emploi des forces nucléaires et autres éléments de forces présentant un caractère très sensible.	Les études sur des sujets sensibles ¹ .
	Les instructions particulières sur l'emploi et les conditions réelles d'emploi des forces.

¹ La plupart des documents de doctrine (NRBC exclu) doivent être connus du plus grand nombre. Ils ne doivent pas être classifiés. A l'instar des dispositions réglementaires ils comporteront la mention DR.

TRÈS SECRET	SECRET
1- <u>QUESTIONS D'ORDRE GÉNÉRAL</u>	
	Certaines études dans les domaines militaires (stratégiques, opératifs, opérationnels et tactiques, techniques) touchant aux concepts d'emploi des forces tant que les réflexions ne sont pas figées.
Certaines synthèses d'études sur les plans à long terme et sur l'organisation des forces, en particulier dans les domaines nucléaire et de la guerre électronique.	Certaines synthèses d'études sur les plans à long terme et sur l'organisation des forces à l'exception du domaine nucléaire et de la guerre électronique.
	La plupart des études sur les plans à long terme.
Certaines recherches scientifiques et techniques qui présentent une importance majeure pour la politique de défense.	Certaines recherches scientifiques et techniques qui présentent une importance pour la politique de défense. Certains documents de synthèse concernant les orientations technologiques.
Certaines données financières susceptibles de dévoiler les intentions gouvernementales et militaires.	Certaines études financières sur les plans d'équipement des forces.
Les accords militaires et protocoles particuliers.	Les accords militaires et protocoles particuliers après concertation avec les autres signataires.
Certains documents concernant les aspects militaires de négociations inter alliées ou internationales.	Certains documents concernant les aspects militaires de négociations inter alliées ou internationales après concertation avec les autres signataires.
Documents se référant explicitement à des documents, concepts et arguments de pays ou organisations alliées ayant la classification <i>Top Secret</i> ou équivalent.	Documents se référant explicitement à des documents, concepts et arguments de pays ou organisations alliées ayant la classification au niveau <i>Secret</i> ou équivalent.
Documents de relations internationales militaires que nos partenaires étrangers souhaitent classer <i>Top Secret</i> ou équivalent.	Documents de relations internationales militaires que les partenaires étrangers souhaitent classer au niveau <i>Secret</i> ou équivalent.
Documents de coopérations internationales que les partenaires étrangers classent ou souhaitent classer <i>Top Secret</i> ou équivalent.	Documents de coopérations internationales que les partenaires étrangers classent ou souhaitent classer <i>Secret</i> ou équivalent.
Mesures d'alerte essentielles aux échelons élevés du commandement touchant au domaine nucléaire et à la guerre électronique.	Mesures d'alerte essentielles aux échelons élevés du commandement à l'exception de celles touchant au domaine nucléaire et de la guerre électronique.

TRÈS SECRET	SECRET
1- <u>QUESTIONS D'ORDRE GÉNÉRAL</u>	
	Mémentos d'alerte.

TRÈS SECRET	SECRET
2 - <u>QUESTIONS RELATIVES AUX OPÉRATIONS</u>	
	Théâtre européen.
	Planification opérationnelle des unités non nucléaires et d'un niveau inférieur aux grands commandements.
	Attributions des autorités chargées d'un grand commandement opérationnel.
	Procédures opérationnelles sauf celles ayant trait aux questions nucléaires.
	Questions relatives à la géographie militaire.
	Études sur les systèmes d'aide au commandement.
	Schémas directeurs.
	Directives initiales de planification et appréciation stratégique.
	Les plans de défense des grands commandements (hors chapitres spécifiques <i>Très Secret</i>).
	Schéma directeur d'opérations.
	Plans d'emploi et plans d'opérations.
	RESEVAC (Plans d'évacuation des ressortissants)
Plans de défense nationaux. – Les plans de recherches, moyens techniques mis en œuvre et certains aspects renseignements.	Logistique : Plans de desserrement éventuels.
Plans directement liés à la sécurité des forces nucléaires.	Plans directement liés à la sécurité des forces nucléaires stratégiques et tactiques après concertation avec les autres signataires.
Plans d'engagement nationaux ou avec les alliés.	Plans d'intervention et de renforcement Outre-mer y compris les aspects relatifs aux plans de défense nationaux et plans de desserrement.

TRÈS SECRET	SECRET
2 - <u>QUESTIONS RELATIVES AUX OPÉRATIONS</u>	
	Ensemble des plans de stationnement et des études sur les stationnements futurs.
	Études de déploiement hors d'Europe.
Documents de synthèse concernant l'organisation du commandement en temps de crise : transmissions, infrastructure, implantation des PC, etc.	
Exercices et manœuvres mettant en œuvre les plans alliés, nationaux, les plans de défense (thèmes généraux, moyens mis en œuvre, dispositifs, modalités de montée en puissance, résultats et appréciations) concernant les forces nucléaires et la guerre électronique.	Exercices et manœuvres mettant en œuvre les plans alliés, nationaux, les plans de défense (thèmes généraux, moyens mis en œuvre, dispositifs, résultats et appréciations) à l'exception du domaine nucléaire et de la guerre électronique.
	Ordres d'opérations concernant les exercices et manœuvres ne faisant pas référence à des plans.
	Planification et synthèses d'exercices.
Emploi de certaines forces rares et sensibles (unités de recherche du renseignement, etc.).	

TRÈS SECRET	SECRET
3 - <u>QUESTIONS RELATIVES AU RENSEIGNEMENT</u>	
Études générales des besoins en renseignement.	
Plans de recherche à l'échelon interarmées ou des états-majors d'armées.	Plans de recherche à l'échelon des grands commandements d'emploi.
	Plans de recherches particularisés à un moyen ou à une source.
Certains ordres de recherche.	La plupart des notes d'orientation.
Certaines synthèses de renseignement sur les puissances étrangères.	La plupart des synthèses de renseignement sur les puissances étrangères.
	Certains documents de diffusion du renseignement.
Certaines études critiques sur des matériels ou des procédés techniques étrangers nouveaux ou importants liés à un plan ou à un ordre d'opération.	La plupart des informations liées au risque de prolifération NRBC des puissances émergentes (mention <i>Spécial France</i>).

TRÈS SECRET	SECRET
3 - <u>QUESTIONS RELATIVES AU RENSEIGNEMENT</u>	
Certains comptes rendus de renseignement.	La plupart des comptes rendus de renseignement.
Certaines informations sur les méthodes employées ou le succès obtenus par les sources secrètes de renseignement et les services de contre-espionnage.	
Certains documents d'étude sur les moyens, le dispositif et les procédures des unités du renseignement militaire et de la guerre électronique.	Certains documents traitant des activités et de l'entraînement des unités et du personnel spécialiste du renseignement.
Dossiers d'objectifs majeurs.	Certains dossiers d'objectifs, d'entraînement, d'exercices ou de simulation.
Renseignements résultant d'une analyse cryptographique quand il n'y a pas de marquage du texte original.	
	Certaines études relatives au moral et au personnel.
Rapports particuliers ou occasionnels sur des sujets pouvant présenter une sensibilité particulière.	Documents de gestion susceptibles de dévoiler des intentions militaires.
	Synthèses partielles (drogue, désertion, antimilitarisme, etc.).

TRÈS SECRET	SECRET
4 - <u>QUESTIONS RELATIVES À LA PROTECTION</u>	
	Directives nationales de sécurité.
	Plan particulier de protection des PIV.
	Plans de sécurité opérateurs.
	Certaines questions d'infrastructure liées à la sécurité des installations ² .

² Se référer au code de l'environnement.

TRÈS SECRET	SECRET
4 – <u>QUESTIONS RELATIVES À LA PROTECTION</u>	
	Rapports d'inspection et comptes rendus d'évaluation ou d'exercices concernant la protection d'un PIV.
Etudes de vulnérabilité, dispositions des mesures et protections militaires face aux menaces de malveillance envers les bâtiments de la marine porteurs de chaufferies ou d'armes nucléaires.	
Certaines questions d'infrastructure telles que projets de centres sensibles et plans d'installation de niveau gouvernemental.	Certaines questions d'infrastructure telles que projets de centres sensibles et plans d'installation de niveau gouvernemental à l'exception de celles relatives au domaine nucléaire et de la guerre électronique.
	Mise en place de certains personnels, matériels, dispositifs de protection.
	Rapports avec les autorités civiles concernant la participation des armées en cas de troubles ou d'événements graves.
Certains dossiers et comptes rendus concernant des atteintes graves à la sécurité de la défense.	Les dossiers relatifs à la sécurité des personnes et certains dossiers et comptes rendus concernant les atteintes à la sécurité de la défense.

TRÈS SECRET	SECRET
5 - <u>QUESTIONS RELATIVES À LA LOGISTIQUE ET À LA MOBILISATION</u>	
Travaux et questions domaniales relatives à des décisions classifiées <i>Très Secret</i> (SSBS, QG nationaux).	
Certains travaux préparatoires aux discussions d'accords logistiques internationaux lorsque la situation politique internationale l'exige.	La plupart des travaux préparatoires aux discussions d'accords ou aux échanges d'informations logistiques internationales.
	La plupart des travaux d'exploitation d'exercices interalliés avec ou sans participation effective des armées.
Certains documents concernant l'aide militaire à des gouvernements étrangers lorsque la situation politique internationale l'exige.	Soutiens logistiques urgents apportés à des armées étrangères.

TRÈS SECRET	SECRET
5 - <u>QUESTIONS RELATIVES À LA LOGISTIQUE ET À LA MOBILISATION</u>	
	La plupart des questions relatives au soutien logistique des forces de présence à l'étranger, des éléments d'assistance rapide des éléments français de forces multinationales et notamment celles traitant de l'organisation du soutien.
	La plupart des travaux concernant les accords passés ou à conclure avec des pays étrangers et liés à une présence militaire française.
Transports de matières nucléaires selon la catégorisation des matières ainsi que des matériels et du personnel dont le déplacement est couvert par une classification particulière.	Transports de matières nucléaires selon la catégorisation des matières. Certains transports d'armement, munitions, matériels sensibles.
	Les plans de remplacement des services publics.
	Certains problèmes logistiques interarmées et notamment ceux relatifs aux stocks de crise et de guerre.
Plans de mobilisation.	Synthèses des plans de mobilisation.
	Catalogue des mesures à prendre.
	Directives et instructions particulières concernant le plan de mobilisation.
	Répertoires généraux relatifs à la mise sur pied des moyens.
Documents de synthèses relatifs à la montée en puissance du personnel.	Analyse de situation sur la montée en puissance (difficultés, actions, lacunes).
	Études particulières sur des vulnérabilités importantes.
Certaines synthèses sur les vulnérabilités des systèmes et des forces.	

TRÈS SECRET	SECRET
6 - <u>QUESTIONS RELATIVES AUX SYSTÈMES NUMÉRIQUES, DE COMMUNICATION ET DE GUERRE ÉLECTRONIQUE</u>	
Certains dossiers de sécurité concernant les centres de traitement de l'information en fonction de leur importance pour le commandement, de leur vulnérabilité et de la sensibilité des informations traitées.	Les dossiers de sécurité relatifs aux sites de traitement de l'information, aux réseaux locaux et aux systèmes d'information et de communication lorsqu'ils intègrent les mécanismes de protection mis en œuvre et les vulnérabilités potentielles.
Les rapports d'audit ou d'analyse lorsqu'ils décrivent les éléments particulièrement sensibles en matière de sécurité, notamment les vulnérabilités, et qu'ils se rapportent à un centre de traitement de l'information (voir <i>supra</i>).	La plupart des rapports d'audit ou d'analyse en matière de sécurité des systèmes numériques, de communication et de guerre électronique. Certains éléments et comptes rendus d'incident SSI (compromissions).
Certains états de vulnérabilité des systèmes ou d'équipements (amis/ennemis).	La plupart des études sur des vulnérabilités des systèmes ou d'équipements (amis/ennemis).
Certaines études relatives aux concepts d'emploi, aux plans d'action opératifs ou stratégiques en matière de maîtrise des systèmes numériques ou de guerre de l'information.	La plupart des plans d'action en matière de maîtrise des systèmes numériques ou de guerre de l'information. Certains plans d'opérations, études et bases de données en matière de maîtrise des systèmes d'information et de communication.
Certains documents de conception détaillée des équipements de guerre électronique et de sécurité des systèmes numériques et de communication.	Les dossiers d'architecture technique de la plupart des équipements de guerre électronique et des équipements de sécurité des systèmes numériques et de communication.
	Les documents de conception de nommage et d'adressage complets des réseaux informatiques.
Certaines clés de chiffrement, les réseaux de chiffrement, les éléments d'identification ou de camouflage et les documents concernant l'alerte.	Les clés de chiffrement, les éléments secrets d'identification ou de camouflage et les documents concernant l'alerte.
Certaines informations de mise en place des moyens de guerre électronique et des clés de chiffrement.	Les informations de mise en place des moyens de guerre électronique et des clés de chiffrement.

Certains plans globaux d'attribution des fréquences (fichiers interarmées d'attribution des fréquences) et plans d'attribution des fréquences « guerre » et d'opérations.	Plans globaux d'attribution des fréquences (fichiers interarmées d'attribution des fréquences) et plans d'attributions des fréquences « guerre » et d'opérations.
---	---

TRÈS SECRET	SECRET
7 - <u>QUESTIONS CONCERNANT LES MATÉRIELS, LES SYSTÈMES D'ARMES ET LES RECHERCHES OU ÉTUDES CORRESPONDANTES</u>	
Certaines synthèses d'étude sur les plans à long terme.	Plans à long terme en matière d'armement.
	Dossiers préparatoires à la programmation budgétaire et à la loi de programmation militaire.
	Programme pluriannuel des recherches et études.
	Certains programmes d'armement et d'infrastructure des armées.
Certaines études d'ordre technique ou d'ordre opérationnel visant à la conception (concepts, modélisation, technologie des systèmes et des matériaux, composants) et à l'évaluation (performances, coûts) des matériels ou systèmes d'armes. Les vulnérabilités critiques des systèmes d'armes.	Certaines études d'ordre technique ou d'ordre opérationnel visant à la conception (concepts, modélisation, technologie des systèmes et des matériaux, composants) et à l'évaluation (performances, vulnérabilité, coûts) des matériels ou systèmes d'armes.
Certaines caractéristiques, certaines performances, certains matériels, certains logiciels en raison de leur sensibilité particulière.	Certaines caractéristiques, performances, disponibilité ou modes d'utilisation des matériels ou des systèmes pouvant constituer un indicateur de capacités militaires.
Certaines caractéristiques du durcissement des systèmes les plus sensibles.	La plupart des caractéristiques de durcissement des systèmes.

TRÈS SECRET	SECRET
7 - <u>QUESTIONS CONCERNANT LES MATÉRIELS, LES SYSTÈMES D'ARMES ET LES RECHERCHES OU ÉTUDES CORRESPONDANTES</u>	
<p>Certaines performances, limitations d'emploi particulièrement sensibles et vulnérabilités des moyens de détection (radars, sonars, détecteurs, IR, autodirecteurs, etc.) ; en particulier celles touchant aux limitations d'emploi et à la vulnérabilité et des capacités de contre-mesures (CME).</p> <p>Les performances, limitations d'emploi et vulnérabilités des contre-contre-mesures électroniques (CCME) des moyens de détection nationaux³.</p>	<p>Certaines performances des moyens de détection (radars, sonars, détecteurs, IR, autodirecteurs, etc.) et capacités de contre-mesures (CME).</p>
<p>Les signatures (EM-IR acoustiques, etc.) des systèmes les plus sensibles.</p>	<p>Tout ou partie des signatures (EM-IR acoustiques, etc.) des systèmes.</p>
<p>Certaines questions touchant des domaines à protéger particulièrement :</p> <ul style="list-style-type: none"> - techniques d'emploi des matériels de guerre nouveaux et importants ; - amélioration de matériels de guerre majeurs ; - armes chimiques et défense biologique ; - armes nucléaires ; - centres d'expérimentation ; - certains systèmes spatiaux ; - moyens et modèles de simulations. 	<p>Certaines études sur les effets des armes nucléaires.</p>
<p>Certaines études spatiales notamment les résultats et synthèses concernant des applications militaires.</p>	
<p>Certaines inventions et demandes de brevets d'invention.</p>	
<p>Certaines directives très importantes à des représentants à l'étranger.</p>	<p>La plupart des directives à des représentants à l'étranger.</p>

³Certaines CCME peuvent être classifiées *Secret* lorsque les partenaires étrangers classent ou souhaitent classer *Secret* ou équivalent et en fonction d'une analyse démontrant l'acceptabilité d'une telle proposition.

ANNEXE 14**ENGAGEMENT DE NON-DIVULGATION DES INFORMATIONS ET
SUPPORTS *DIFFUSION RESTREINTE*****ATTESTATION DE RECONNAISSANCE DE RESPONSABILITÉ ET DE
NONDIVULGATION DES INFORMATIONS ET SUPPORTS PORTANT LA MENTION
*DIFFUSION RESTREINTE***

NOM et PRENOM :

Grade ou fonction :

Service employeur :

Je reconnais être dûment informé des responsabilités et obligations qui m'incombent :

- au titre de la protection des intérêts fondamentaux de la nation et plus particulièrement au titre des dispositions des articles 410-1 et suivants du code pénal relatives à l'espionnage et à la trahison et aux atteintes au secret de la défense nationale ;
- au titre des mesures de sécurité déclinées par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, notamment son paragraphe 1.4.3, ainsi que son annexe 1 ;
- *pour les fonctionnaires ou agents contractuels* : au titre de la discrétion et du secret professionnel en application des articles L.121-6 et L.121-7 du code général de la fonction publique ;
- *pour les militaires* : au titre du statut général des militaires en application de l'article L.4121-2 du code de la défense.

En conséquence, je m'engage sans réserve :

- à ne pas divulguer, par quelque moyen que ce soit, les informations et supports portant la mention *Diffusion Restreinte* à des personnes physiques ou morales n'ayant pas le besoin d'en connaître ;
- à faire preuve de rigueur dans la gestion des informations et supports portant la mention *Diffusion Restreinte* que je serai amené à traiter.

À [Lieu], le [date]

Signature de l'intéressé

ANNEXE 15

FICHE DE POSITION

Référence du document

N°.....en date du.....

Exemplaire n°

Niveau de classification

Détenteur :

Nom Prénom

Emprunté le	Identité de l'emprunteur	Emargement emprunteur	Restitué le	Emargement détenteur

ANNEXE 16

CAHIER D'ENREGISTREMENT DU COURRIER CLASSIFIÉ

Arrivée :

Références du document (S)		Echéance de classification	PCS de rattachement ²⁷⁶	n° BE (A, B, B')	destinataire	émargement	Pièce / Armoire forte	observations
n° de courrier arrivé	origine date							
15411	ARM/EMAT 24/08/1970	24/08/2020	=		COL B.		Coffre n°1	
25412	EMA/SSA 28/02/1990	28/02/2030			Arza M.		Coffre n°2	
15487 Détruit le 29/01/2021 PV 2021-05/ARM/ ...	DGA/DSA/SP 14/12/2001				Durant F.		Pièce n° 1	
25413	EMA/OIA/COS 30/06/1976	30/06/2021			Pierrot D.		Pièce 1010 Coffre n°2	

Références du document (TS)			Echéance de classification	PCS de rattachement ³⁰⁸	n° BE (A, B, B')	destinataire	émargement	Pièce / Armoire forte	Observations
n° de courrier arrivé	n° d'exemplaire	origine date							
15920		ARM/D PID 28/07/1987	28/07/2037			Tief E.		Coffre n°2	
15921		DEF/EM AT/BTS D 21/05/1968	21/05/2018			COL X.		Pièce 1009 Coffre n°1	

²⁷⁶ Ne s'adresse qu'aux personnes morales liées par contrat ou convention avec le ministère de la défense.

Départ :

Références du document S		Echéance de classification	PCS de rattachement	n° BE (A, B, B')	destinataire	Pièce / Armoire forte	Observations
n°	origine						
254	SteX/BCA	21/01/2021		35/01	DGA		
				36/01	SteY		
					Archive OST	coffre	

Références du document TS		Echéance de classification	PCS de rattachement	n° BE (A, B, B')	EX. n°	destinataire	Pièce / Armoire forte	Observations
n°	origine							
<u>14/19</u> 19/19	SteX/BCA SteX/BSD	25/01/2021		41/01	1/3	DGA		
				42/01	2/3	SteY		
					3/3	Archive OST	coffre	

ANNEXE 17

INVENTAIRE CONTRADICTOIRE

Lieu, le

N° -----/Timbre/Classification

PROCÈS VERBAL D'INVENTAIRE CONTRADICTOIRE
DE DOCUMENTS CLASSIFIÉS DE NIVEAU S – TS

Date de l'inventaire : JJ/MM/AAAA

Inventaire contradictoire réalisé à l'occasion du changement de titulaire / Inventaire annuel

Nom, grade et fonction du détenteur responsable (descendant) :

Grade Nom Prénom, fonction

Nom, grade et fonction du détenteur responsable (montant) :

Grade Nom Prénom, fonction

Nombre de documents classifiés : XX

Nombre de supports numériques classifiés : XX

Numéro du doc.	Timbres	Date du document	N° d'ex.	Intitulés si non classifiés ou PCS concerné
		XX/XX/XXXX	XX/XX	Instruction XXXXXXXXXXXX

Type de support	Référence du support	Nombre de documents/ (Mo/Go)

Détenteur responsable (descendant) :

Grade Nom prénom

Détenteur responsable (montant) :

Grade Nom prénom

DESTINATAIRE(S) :

- Officier de sécurité
- détenteur

ANNEXE 18

**DEMANDE DE DESTRUCTION D'INFORMATIONS ET SUPPORTS
CLASSIFIÉS *TRES SECRET****Ministère**Organisme employeur**(timbre)**N° ... /***DEMANDE DE DESTRUCTION
DE SUPPORTS CLASSIFIÉS
*Très Secret*****Support classifié *Très Secret* dont la destruction est demandée :**

- Références :

- numéro d'enregistrement et timbre :

- date de création :

- Numéro de l'exemplaire dont la destruction est envisagée :

Organisme demandeur :**Motif succinct de la demande :**
.....**Sauf avis contraire, j'envisage de procéder à la destruction du support. Aussi, sans réponse dans un délai de deux mois, je procèderai à la destruction du support et vous en rendrai compte en vous adressant une copie du procès-verbal.**

À, le

*Nom, qualité, signature de l'autorité responsable de la demande
cachet de l'organisme.***Destinataires :**

ANNEXE 19

MESURES CONSERVATOIRES ET CONDUITE À TENIR EN CAS DE COMPROMISSION POSSIBLE AFFECTANT UN SYSTÈME NUMÉRIQUE

1. Principes généraux

Il convient de mettre en œuvre des dispositions organisationnelles permettant au plus tôt de :

- préserver le support numérique susceptible de contenir une compromission ;
- rassembler les éléments techniques et humains en rapport avec l'incident en cours ;
- informer la DRSD qui prend en charge les investigations.

Rappel :

Toutes les actions entreprises entrent dans le cadre d'une première réponse sur incident. Elles doivent impérativement être répertoriées et horodatées.

Toute intervention (visualisation du contenu d'un message, fichier ou répertoire, etc.) sur la machine est de nature à laisser des traces sur le disque dur et ainsi à compromettre la recevabilité judiciaire de la preuve.

Aussi, dès la découverte d'une compromission possible, seules les interventions techniques dûment mandatées par la DRSD sont autorisées.

2. Règles de base applicables par l'organisme touché par une compromission possible (officier de sécurité des systèmes d'information ou officier de sécurité)

a. Compromission possible sur une machine isolée

Si l'équipement est en fonctionnement :

- laisser la machine en fonctionnement ;
- ne pas retirer les médias amovibles connectés, s'il y en a.

Si l'équipement a été éteint, ne pas rallumer la machine.

b. Compromission possible sur une machine connectée au réseau :

Appliquer les mêmes dispositions que celles prévues pour une machine isolée (§2.a).

En complément :

- noter le numéro de la prise murale du réseau ;
- débrancher le câble à l'arrière de celle-ci ;
- demander aux administrateurs du système de mettre à disposition de la DRSD les journaux d'événements des différents équipements liés (serveurs, commutateurs, etc.).

3. Premières constatations et investigations

Au-delà des règles de base ci-avant, les premières constatations et les investigations ultérieures doivent être réalisées par un inspecteur de la DRSD dès qu'une suspicion de compromission affectant un système numérique est signalée.

ANNEXE 20

DOCUMENTS TRAITANT D'INFORMATIONS ET SUPPORTS CLASSIFIÉS À L'INTERNATIONAL

1. Accord général de sécurité

Un accord général de sécurité est élaboré dès l'instant où les échanges d'informations et supports classifiés avec l'étranger impliquent plusieurs ministères. Cet accord, bilatéral ou multilatéral, engage les gouvernements concernés. Les accords qui fixent les règles de sécurité applicables à une organisation internationale et aux pays qui y adhèrent entrent dans cette catégorie des accords généraux de sécurité. Ces accords ont valeur de traités internationaux.

En tant qu'autorité nationale de sécurité, le SGDSN est responsable de l'élaboration et de la mise en application de ces accords. Il détermine les priorités pour leur établissement en lien avec le ministère de la défense (DAJ, DGA, DRSD, EMA). Le service du HFCDS est tenu informé de ces travaux.

Le SGDSN mène les négociations avec la partie étrangère en y associant, en tant que de besoin, pour le ministère de la défense, la DAJ, la DGA, et l'EMA.

Ces accords définissent en particulier :

- les équivalences des niveaux de protection entre les pays concernés par l'accord ou éventuellement les modalités pour les définir ou pour y déroger ;
- les conditions d'accès aux informations et supports classifiés générées en commun ou échangées ;
- leurs modes de transmission ;
- les modalités d'habilitation des personnes physiques et morales nécessaires pour les échanges ou l'exécution des contrats en coopération ;
- les modalités de gestion, reproduction, traduction et destruction des informations classifiées, le cas échéant ;
- les modalités relatives aux échanges d'informations dans le cadre de contrat classifiés ;
- les règles en matière de visites ;
- les mesures à prendre en cas d'atteinte à la sécurité.

Ils sont établis après analyse et comparaison des réglementations respectives sur la protection du secret de la défense nationale.

La signature d'un accord de sécurité avec un partenaire étranger engage celui-ci à protéger les informations et supports classifiés français et protégés (*Diffusion Restreinte*), communiqués ou échangés, selon des dispositions équivalentes à celles appliquées pour ses propres informations et supports classifiés de même niveau ou selon les dispositions spécifiées par l'accord de sécurité. Par réciprocité, le gouvernement français s'engage à assurer aux informations et supports classifiés d'origine étrangère une protection équivalente à celle appliquée aux informations françaises de même niveau ou selon les dispositions spécifiées par l'accord de sécurité.

La publication d'un tel accord rend celui-ci opposable aux tiers et permet tout recours et application des sanctions prévues au code pénal.

La DRSD est compétente pour conduire les inspections relevant du ministère dans les organismes ou établissements qui détiennent des informations et supports classifiés transmis par un partenaire étranger. Des audits en sécurité de défense sont aussi conduits par la DGA en tant qu'autorité de sécurité déléguée dans son domaine de compétences pour s'assurer de la mise en œuvre des dispositions des accords de sécurité et des documents spécifiques (instruction de sécurité programme, plan contractuel de sécurité internationale) et vérifier la protection et la manipulation des informations et supports classifiés des partenaires étrangers et des organisations internationales confiés à la France.

L'autorité nationale de sécurité effectue également des audits (ou inspections), notamment pour le sous-réseau COSMIC.

2. Accord de sécurité dans le domaine de la défense ou de l'armement

Lorsque les échanges concernent un ensemble de domaines particuliers qui relèvent du ministère, ou lorsqu'il n'est pas possible d'identifier l'autorité nationale de sécurité étrangère compétente, un accord de sécurité dans le domaine de la défense ou plus spécifiquement de l'armement peut remplacer un accord général de sécurité. Dans certains cas, un accord de sécurité dans le domaine de la défense ou de l'armement peut être conclu en sus d'un accord général de sécurité lorsque le partenaire étranger dispose d'une autorité nationale de sécurité civile et d'une autorité nationale militaire et qu'il existe des règles étrangères propres au domaine militaire.

Au sein du ministère, la DAJ prépare et négocie ces accords, en concertation avec la DGA, l'EMA, le SGDSN et le ministère des Affaires étrangères. Il s'agit d'un traité ou d'un accord intergouvernemental qui engage l'État ou le gouvernement, le partenaire étranger, dans le domaine précisé par l'accord (défense et/ou armement). Il est établi selon les mêmes principes et comprend les mêmes types d'engagements qu'un accord général de sécurité.

La liste des accords généraux, de défense ou d'armement est tenue à jour par la DAJ (DIE/I).

3. Projets, programmes ou contrats en matière d'armement

Accord intergouvernemental sous forme d'échange de lettres ou de notes

En l'absence d'accord de sécurité, dans le cas d'échanges portant sur un domaine spécifique donné, un projet ou un contrat export, un échange de notes ou de lettres peut permettre la transmission ou l'échange d'informations et supports classifiés. Cet échange, rédigé pour des sujets spécifiques, sensibles, ne peut pas reposer sur un tableau d'équivalence de classifications, ni ne prévoir de double marquage, mais décrit alors les mesures de protection à prendre par la partie destinataire pour les informations et supports classifiés français. En France, le pilote de la rédaction est le SGDSN qui peut déléguer à une autorité de sécurité déléguée. Les clauses sont définies en fonction de la nature du projet, de sa sensibilité et du contexte local.

Sous le contrôle de l'autorité de sécurité compétente (ANS ou ASD), en fonction des clauses mentionnées dans l'accord, les attestations, les certificats de courriers et les plans de transport mentionnés à l'annexe 20 sont possibles.

Dispositions particulières de sécurité

En l'absence d'accord de sécurité, dans le cas d'échanges portant sur un domaine spécifique donné, un projet ou un contrat armement, l'établissement de dispositions particulière de sécurité (DPS) peut permettre la transmission ou l'échange d'informations classifiées. Les dispositions particulières de sécurité est matérialisée par un échange de lettres au niveau des ministres de la défense. Elles fixent les exigences de protection et de manipulation des informations et supports classifiés échangés pour le domaine, projet, contrat export concerné. En particulier, la lettre envoyée par le ministre de la défense demande au ministre étranger de s'engager, au nom de son gouvernement, à assurer aux informations protégées de défense relatives à ces équipements un niveau de protection au moins équivalent à celles dont elles bénéficient sur le territoire français. Cette lettre est accompagnée d'un document exposant les principales dispositions de la législation française sur la protection du secret de la défense nationale, auquel est joint un projet de réponse destiné à être signé par le ministre étranger.

Ces documents sont préparés par la DGA, revues par la DAJ et transmises au cabinet du ministre pour l'envoi au ministre étranger concerné. Celui-ci est alors responsable de l'application de ces dispositions particulières. La liste de ces dispositions est tenue à jour pour le ministère de la défense par la DGA et transmise pour information au SGDSN. Elle possède la mention Diffusion Restreinte et est accessible uniquement sur demande.

Lorsque de l'information est uniquement échangée au niveau DR et dans le cas où le cadre mis en place des dispositions particulières de sécurité, un plan contractuel de sécurité international (PCSI) est établi.

Les attestations internationales de sécurité, les certificats de courriers et les plans de transport mentionnés à l'annexe 20 sont possibles et selon les mêmes modalités.

Assurance de sécurité

Cette notion relève des réglementations OTAN²⁷⁷ et OCCAR²⁷⁸.

Les contrats avec des titulaires établis dans des pays non OTAN, ou non OCCAR (ci-après désignés organisations internationales – OI) qui impliquent des informations et supports classifiés de ces organisations internationales requièrent l'existence d'un accord de sécurité ou d'un arrangement bilatéral entre l'OI et le pays non OI dont l'autorité nationale de sécurité ou l'autorité de sécurité déléguée a juridiction sur les titulaires. Il incombe à cette autorité nationale de sécurité ou autorité de sécurité déléguée de faire en sorte que les titulaires assurent le niveau de protection requis pour les contrats impliquant l'accès ou la détention d'informations et supports classifiés de l'OI.

En l'absence d'un accord de sécurité bilatéral entre l'OI et le pays non OI concerné, et pour échanger des informations et supports classifiés de l'OI, il faut qu'un accord de

²⁷⁷ C-M(2002)49-COR12.

²⁷⁸ OMP 11_OCCAR Security Regulations.

sécurité bilatéral existe ou soit conclu entre un pays membre de l'OI contractant et le pays non OI et que ce pays OI contractant se porte garant²⁷⁹.

Le pays membre de l'OI qui se porte garant remet à l'OI une assurance de sécurité écrite signée par un représentant dûment mandaté par le destinataire non OI. L'assurance de sécurité oblige le destinataire non OI à assurer aux informations OI classifiées un niveau de protection au moins égal à celui des dispositions contenues dans l'accord de sécurité bilatéral pour la protection des informations et supports classifiés du pays membre de l'OI d'un niveau de classification équivalent.

Plan contractuel de sécurité international

La description détaillée du contenu et de la portée des plans contractuels de sécurité est précisée à la fiche 9.3 de la présente instruction.

4. Instruction de sécurité de programme

Lors de la mise en place d'un programme en coopération, l'accord intergouvernemental ou l'arrangement technique ou administratif, fixe les clauses générales de sécurité, applicables à ce programme, dans le droit fil de l'accord de sécurité et précise le besoin de rédaction d'une instruction de sécurité programme (ISP) pour décliner et préciser les règles de sécurité.

L'instruction de sécurité programme, dont la rédaction est pilotée par la direction de programme (nationale, du partenaire ou leur équivalent pour les organisations internationales) avec le support de leur autorité de sécurité, fixe les règles de protection communes des informations concernant cette coopération. Une instruction de sécurité programme contient un guide de classification dûment protégé.

Cette instruction de sécurité programme est validée, pour la France, par la DGA, en tant qu'autorité de sécurité déléguée pour son périmètre de compétence dans le domaine de l'armement, ou par l'EMA pour les coopérations à vocation opérationnelle.

Dans le cadre des contrats, l'instruction de sécurité programme est déclinée en France en plans contractuels de sécurité nationaux ou internationaux ou le cas échéant selon le modèle approuvé par les pays participant au programme (OCCAr, EDIR/FA, GMSI²⁸⁰, etc.) ou opération en coopération internationale. Ce plan contractuel de sécurité est désigné, dans le cadre international, par l'expression « Security Aspect Letter²⁸¹ » (ou SAL) ou « security annex ».

Lorsque les titulaires sont identifiés dans l'instruction de sécurité programme, et que celle-ci est mentionnée au contrat, elle peut alors être utilisée comme plan contractuel de sécurité (national ou international)²⁸². Ces titulaires doivent alors faire partie de la diffusion nominale de l'instruction de sécurité programme.

Une instruction de sécurité programme peut, le cas échéant, être mise en place pour les programmes export complexes.

²⁷⁹ Notion internationale de *sponsorship* (fr. parrainage).

²⁸⁰ Groupe Multilatéral de sécurité Industrielle (groupe informel qui établit des documents de sécurité), aussi dénommé MISWG pour l'acronyme anglais de Multinational Security Working Group.

²⁸¹ Terminologie OTAN.

²⁸² C'est le cas pour certains contrats passés par l'OCCAr au maître d'œuvre principal d'un programme, ou également pour le programme OTAN du NH90.

Les instructions de sécurité programme sont transmises pour information à la DRSD.

5. Arrangement technique ou administratif et arrangement de non divulgation

Des arrangements techniques (AT) ou administratifs peuvent être élaborés pour encadrer une coopération. Les modalités relatives à la protection des informations classifiées ne peuvent pas être créées par un AT et toute stipulation relative au traitement des informations classifiées doit obligatoirement renvoyer au cadre juridique existant entre les parties (constitué par l'accord de sécurité). Un AT peut seulement venir préciser, sans les contredire, certaines dispositions de l'accord de sécurité, pour la coopération qu'il encadre, tant que lesdites précisions entrent dans le champ de compétence du ministre. Un AT peut également indiquer le niveau de classification requis pour l'échange des informations classifiées dans le cadre de la mise en œuvre de ladite coopération.

Dans certains cas, notamment lorsqu'une coopération en matière d'armement est envisagée ou prévue, un arrangement de non divulgation (*Non disclosure arrangement*) peut être signé. Lorsqu'il existe un accord de sécurité, l'arrangement de non divulgation porte sur les informations classifiées et sensibles. Concernant les informations classifiées et protégées, l'arrangement de non divulgation renvoie au cadre juridique existant (constitué par l'accord de sécurité). Concernant les informations sensibles, qui ne sont pas des informations classifiées ou protégées, il encadre l'échange de ces informations, les règles en matière de non-divulgence et de suivi, sécurité et destruction. Lorsqu'il n'existe pas d'accord de sécurité, l'arrangement de non divulgation porte uniquement sur les informations sensibles.

6. Attestations internationales de sécurité

Ces attestations sont communément utilisées entre la France, les pays signataires d'un accord de sécurité, et les organisations internationales.

Il existe trois formulaires types :

Facility Security Clearance Information Sheet (FSCIS)

Littéralement « feuille d'information d'habilitation d'un établissement », ce document, validé par les autorités nationales de sécurité ou autorités de sécurité déléguée, sert à informer sur le niveau d'habilitation d'un établissement d'une personne morale, son aptitude physique et sa capacité à traiter de l'information numérique mais aussi, si demandé, à initier une procédure d'habilitation.

Ce document est renseigné par l'officier de sécurité de l'organisme demandeur (étatique ou privé) et transmis à son autorité nationale de sécurité ou autorité de sécurité déléguée pour traitement. Il est ensuite transmis à l'autorité nationale de sécurité ou autorité de sécurité déléguée homologue dont ressort la personne morale objet de la requête pour réponse vers l'autorité nationale de sécurité ou l'autorité de sécurité déléguée requérante.

Personnel Security Clearance Information Sheet (PSCIS)

Littéralement « feuille d'information d'habilitation d'une personne », ce document validé par les autorités nationales de sécurité ou autorités de sécurité déléguées, sert à informer sur le niveau d'habilitation d'une personne physique mais aussi, si demandé, à initier une procédure d'habilitation.

Ce document est renseigné par l'officier de sécurité de l'organisme demandeur (étatique ou privé) et transmis à son autorité nationale de sécurité ou autorité de sécurité déléguée pour traitement. Il est ensuite transmis à l'autorité nationale de sécurité ou autorité de sécurité déléguée homologue du pays du ressortissant objet de la requête pour réponse vers l'autorité nationale de sécurité ou autorité de sécurité déléguée requérante.

Personnel Security Clearance Assurance Request (PSCAR)

Littéralement "demande d'attestation de sécurité d'une personne ", ce document sert à compléter l'enquête de sécurité d'un individu ayant vécu à l'étranger lorsque le temps de présence de l'individu sur le territoire n'est pas suffisant pour les besoins de l'enquête (règle otanienne des 5 ans notamment), aux fins de savoir qu'il n'y a pas d'information défavorable sur l'intéressé qui empêcherait la délivrance d'une habilitation de sécurité nationale par le pays demandeur.

Le document est complété par l'OS de l'entité privée ou étatique requérante à la demande de l'autorité d'habilitation.

Il est adressé par l'autorité nationale de sécurité ou autorité de sécurité déléguée dont relève la partie requérante à l'autorité nationale de sécurité ou autorité de sécurité déléguée du pays d'origine, ou du pays de dernière résidence de la personne impliquée, qui le complète et le valide et le retourne à l'autorité nationale de sécurité ou autorité de sécurité déléguée requérante.

Ce processus peut aussi être utilisé pour un ressortissant pour constituer l'équivalent d'un contrôle élémentaire par exemple pour pouvoir entrer sur des sites sensibles ou mener des activités qui ne nécessitent pas une habilitation.

Ces formulaires sont disponibles sur le site Internet Armement.

7. Certificat de courrier

Le certificat de courrier est destiné au porteur, habilité ou ayant la qualité de convoyeur autorisé, chargé du transport du courrier, pour attester auprès des autorités de la police des frontières et des douanes du caractère officiel du transport des documents, équipements ou composants couverts par le certificat. Il est utilisé pour éviter les inspections directes des éléments convoyés par le porteur ou, si une inspection est inévitable, obtenir qu'elle soit effectuée dans des conditions de sécurité satisfaisantes, telles que décrites dans le formulaire (par exemple, dans une zone hors de vue des personnes qui n'ont pas une nécessité d'accès aux informations et en présence du convoyeur ou porteur autorisé).

Le recours à un certificat de courrier peut être envisagé comme une alternative à d'autres procédures d'acheminement (valise diplomatique), dès lors que les informations et supports ne comportent pas la mention SF. L'emploi du certificat de

courrier nécessite qu'il y ait un accord de sécurité, un accord par échange de lettres ou de notes ou des DPS.

L'utilisation d'un certificat de courrier pour le transport d'informations et supports classifiés est autorisée entre la France et un ou plusieurs pays coopérant à un projet, un programme ou un contrat (en phase pré-contractuelle ou contractuelle), que ce soient des entités de droit public ou privée.

Le certificat de courrier peut être utilisé pour le convoyage d'informations et supports classifiés à l'étranger dans le cadre d'une opération extérieure, d'un exercice multinational, d'une mission en isolé. Les informations et supports classifiés transportés doivent être accompagnés en permanence par un porteur autorisé.

Il existe deux types de certificats de courrier :

- le certificat de courrier « monovoyage », utilisable pour un seul transport. Un aller et retour avec les mêmes documents équivaut à un seul transport (cf. IGI 1300 – annexe 43) ;
- le certificat de courrier « multivoyages », permettant au porteur d'effectuer plusieurs transports (plusieurs aller et retour entre l'expéditeur et le destinataire) pendant une période de temps donnée (cf. IGI 1300 – annexe 44).

Les certificats de courrier sont délivrés par chaque autorité de sécurité déléguée dans leurs domaines respectifs de compétence. Les autres certificats de courrier n'entrant pas dans ce domaine sont signés par le SGDSN en tant qu'autorité nationale de sécurité. Les têtes de chaîne protection du secret se coordonnent avec le SGDSN pour les certificats de courrier et les plans de transport.

Sont exclus du domaine d'utilisation du certificat de courrier en raison de ses limites d'emploi :

- les documents, équipements ou composants classifiés de l'OTAN ; dans ce cas, le certificat de courrier est remplacé par un document établi selon les dispositions des directives OTAN ;
- sauf dérogation, les documents marqués *Spécial France*²⁸³.

Les limites d'emploi du certificat de courrier sont :

- le certificat de courrier ne confère pas au porteur l'immunité diplomatique au sens de la convention de Vienne (le courrier peut donc être ouvert en douane) ;
- la procédure de transport avec de tels certificats ou une procédure autorisant ces transports est prévue au sein d'un accord de sécurité ou d'un règlement international de sécurité ;
- les certificats de courrier relatifs au transport des articles contrôlés de la sécurité des systèmes d'information font l'objet de directives particulières.

Conditions de choix des porteurs autorisés :

- les porteurs autorisés sont des salariés permanents de l'entité expéditrice ou de la société de transport qui a un contrat avec l'entité expéditrice (notamment dans le cas des courriers référencés par un plan de transport. Il n'est en aucun cas fait appel à des intérimaires, à des transitaires ou à leur personnel, ou à des courriers indépendants ;

²⁸³ Une dérogation est possible pour les entités subordonnées à l'autorité du ministre. La demande doit être adressée par les officiers de sécurité de niveau 1 auprès de l'ANS.

- les porteurs autorisés font l'objet d'une décision d'admission aux informations et supports classifiés de niveau au moins égal à celui des informations à convoier ;
- ces porteurs sont désignés par le chef d'entité et mentionnés dans le certificat de courrier.

Modalités de délivrance du certificat de courrier :

- toute demande de certificat de courrier, signée par l'autorité nationale de sécurité ou l'autorité de sécurité déléguée uniquement est formulée par écrit et transmise à l'autorité de délivrance compétente ;
- cette demande, dûment justifiée par l'officier de sécurité de l'établissement expéditeur, comporte les renseignements indispensables à l'édition du certificat de courrier ;
- la nationalité des porteurs ne peut être différente de celles d'un des pays émetteur et destinataire.

8. Plan de transport

Lorsque le contrat prévoit le transport transfrontalier de matériel classifié en tant que fret, les dispositions suivantes sont prises en compte :

- le degré de protection accordé à un envoi est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient ;
- la société assurant le transport possède une habilitation du niveau approprié, sauf exception justifiée auprès de l'autorité nationale de sécurité ou l'autorité de sécurité déléguée. Dans tous les cas, le personnel accompagnant l'envoi est habilité au niveau approprié et muni d'un certificat de courrier conforme aux dispositions de l'IGI 1300 ;
- avant tout transfert de matériel classifié, un plan de transport est dressé par l'expéditeur et approuvé par les autorités nationale de sécurité ou autorités de sécurité déléguée compétentes. Le modèle de plan de transport à utiliser va dépendre du cadre duquel relève ce transport classifié (OTAN, UE, OCCAR, bilatéral) ;
- les trajets sont aussi directs et rapides que les circonstances le permettent.

Chaque chaîne de protection du secret est responsable de la stratégie de signature²⁸⁴ des plans de transport, des conditions et des modalités de mise en place et de l'utilisation des autorisations de transport relevant de sa compétence ainsi que du contrôle des autorisations délivrées.

Pour le domaine de la coopération, export ou sous-traitance armement, les plans de transport sont approuvés par l'autorité de sécurité déléguée (DGA) qui les transmet à ses homologues des pays traversés et du pays destinataire.

Modalités de délivrance du plan de transport :

- toute demande de plan de transport est formulée par écrit et transmise à l'autorité de délivrance compétente ;

²⁸⁴ En particulier de définir les autorités compétentes du partenaire qui peuvent valider un plan de transport.

- cette demande, dûment justifiée par l'officier de sécurité de l'établissement expéditeur, comporte les renseignements indispensables, requis dans l'instruction éditée par l'autorité, à l'édition du plan de transport.

ANNEXE 21

DURÉE ET MODALITÉS DE CONSERVATION DES DOCUMENTS DE GESTION EN PROTECTION DU SECRET

	DOCUMENT	RESPONSABLE DE LA CONSERVATION	DURÉE DE CONSERVATION
HABILITATION	NIS	Service enquêteur	Version numérique du service enquêteur : pour une durée limitée à ce qui est nécessaire ²⁸⁵ . Version de l'autorité d'habilitation : détruite au plus tard 1 an après la fin de validité de l'AS.
	Avis de sécurité (AS)	Service enquêteur	Version numérique du service enquêteur : pour une durée limitée à ce qui est nécessaire. Version de l'autorité d'habilitation : est détruite au plus tard 1 an après la fin de validité de l'AS.
	Attestation de MEE/MEG	Autorité d'habilitation	Version numérique : pour une durée limitée à ce qui est nécessaire. Version papier : à détruire au plus tard 1 an après la fin de validité de l'AS.
	Engagement de responsabilité (EDR) - Volets 1 et 2	Autorité d'habilitation	Version numérique : pour une durée limitée à ce qui est nécessaire.
	Décision d'habilitation (décision, refus, abrogation)	Autorité d'habilitation	Version papier : à détruire au plus tard 1 an après la fin de validité de l'habilitation. Version numérique : pour une durée limitée à ce qui est nécessaire.
	Récépissé de refus/abrogation d'une habilitation	Autorité d'habilitation	Version numérique : pour une durée limitée à ce qui est nécessaire.
	Décision d'accès aux articles contrôlés de la sécurité des systèmes d'information	Officier de sécurité des systèmes d'information	6 ans après signature de l'EDR2.

²⁸⁵ Elle doit être appréciée au cas par cas et limitée dans le temps au strict nécessaire.

	DOCUMENT	RESPONSABLE DE LA CONSERVATION	DURÉE DE CONSERVATION
DONNÉES CADIVS	Données de traçabilité des accès (SI)	Autorité d'homologation ou autorité d'emploi	1 an : <i>Diffusion Restreinte</i> ou sensible. 3 ans : S. 5 ans : TS.
	Données d'enregistrement contrôle d'accès, détection d'intrusion et vidéo-surveillance (CADIVS) ²⁸⁶	Autorité d'homologation ou autorité d'emploi	Pour le contrôle d'accès et pour les systèmes de visualisation des plaques d'immatriculation : durée d'un an à compter de la date de péremption de l'autorisation. Pour la vidéosurveillance et l'interphonie : durée ne pouvant excéder un mois avec une possibilité d'archiver les images enregistrées pour une durée n'excédant pas un an
	Registre de traçage d'entrée et de sortie	Autorité d'homologation ou autorité d'emploi	Au moins 1 an et au maximum 3 ans.
	Journalisation (conservation en mémoire des événements)	Autorité d'homologation ou autorité d'emploi	Au moins 1 an et au maximum 3 ans.
VIE DES INFORMATIONS ET SUPPORTS CLASSIFIÉS ET DES SYSTÈMES NUMÉRIQUES	RÈGLES GÉNÉRALES		
	Enregistrement (Registre)	BPS/secrétariat de l'organisme	Jusqu'à destruction ou reversement du dernier document figurant dans le registre. À verser ensuite au service d'archives.
	Transport (Bordereaux ABB')	BPS/secrétariat de l'organisme	5 ans après sa date d'édition ou à la destruction du document.
	PV de destruction	BPS/secrétariat de l'organisme	Pour une durée limitée à ce qui est nécessaire, minimum 5 ans (cf. fiche 7.13).
	Inventaire	BPS/secrétariat de l'organisme	10 ans
	PV d'inventaire contradictoire	BPS/secrétariat de l'organisme	10 ans

²⁸⁶ Arrêté du 5 avril 2023 autorisant la mise en œuvre de traitements automatisés de données à caractère personnel relatifs aux systèmes de vidéosurveillance et de contrôle d'accès aux locaux et emprises relevant du ministère de la défense.

	DOCUMENT	RESPONSABLE DE LA CONSERVATION	DURÉE DE CONSERVATION
VIE DES INFORMATIONS ET SUPPORTS CLASSIFIÉS ET DES SYSTÈMES NUMÉRIQUES	INFORMATIONS ET SUPPORTS CLASSIFIÉS PHYSIQUES/ ARTICLES CONTRÔLÉS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION		
	Support (clé USB, DD, document, etc.)	Officier de sécurité	Le support peut être détruit lorsqu'il n'est plus utile pour les supports classifiés au niveau <i>Secret</i> , et après sollicitation de l'émetteur, pour les supports classifiés au niveau <i>Très Secret</i> .
	Registre	Officier de sécurité / officier chiffre pour les ACSSI	Jusqu'à destruction ou reversement du dernier support physique figurant dans le registre. À verser ensuite au service d'archives.
CONTRATS	Historique des contrats	Autorité contractante et service enquêteur	Autorité contractante : 10 ans après la fin du contrat Service enquêteur : 3 ans après la fin du contrat

ANNEXE 22

CATÉGORISATION DES SYSTÈMES NUMÉRIQUES

Un système de catégorisation est constitué d'une liste de catégories de systèmes numériques, de critères de catégorisation à appliquer à ces systèmes, ainsi que d'un processus de catégorisation associé.

Le système de catégorisation des systèmes numériques retenu par un organisme doit être adapté au nombre et à la nature de ses systèmes numériques ainsi qu'à la nature et à la sensibilité de ses missions. Le système de catégorisation proposé infra est un exemple.

Quel que soit le système de catégorisation retenu, les systèmes d'information d'importance vitale (SIIV) devront être individuellement identifiés selon les critères définis dans les textes réglementaires concernés.

Critères de catégorisation

- **L'exposition** d'un système numérique se mesure par le nombre de points d'entrée et de chemins d'attaque ouverts à un attaquant. L'exposition est directement liée au nombre d'interactions avec d'autres systèmes numériques et à l'accessibilité depuis des milieux plus ou moins maîtrisés. En revanche, elle est réduite par un isolement des réseaux mais aussi grâce à la sécurisation de l'environnement du système numérique (réseau support, hébergement et politiques de sécurisation associées, organisation de la SSI, sensibilisation, sécurité physique, etc.). Ainsi, un système numérique hébergé dans un environnement sécurisé et conforme aux exigences de cet environnement présentera une surface d'attaque maîtrisée pouvant limiter ainsi la complexité des études de risques.
- **La criticité** d'un système numérique est directement liée à l'impact qu'une attaque ou un dysfonctionnement pourrait avoir sur les missions et les activités de la personne morale et celles de l'autorité contractante, les personnes et les biens. Elle prend en compte la sensibilité ou la classification des informations, la nature des données traitées (données à caractère personnel, données médicales, etc.). Un système est considéré comme critique si la compromission par un attaquant pourrait produire sur l'entité ou l'autorité contractante des impacts jugés inacceptables.

Catégories de systèmes numériques

- **Systèmes d'information d'importance vitale** : les systèmes d'information et de communication et les services numériques qualifiés d'importance vitale au sens des articles L.1332-6-1 et R.1332-41-2 du code de la défense. La liste des SIIV est mise à jour annuellement.
- **Systèmes numériques essentiels ou névralgiques** : les systèmes d'information et de communication et les services numériques combinant un caractère critique ET un niveau d'exposition élevé.
- **Systèmes importants** : les systèmes d'information et de communication et les services numériques ayant un caractère critique OU un niveau d'exposition élevé.
- **Systèmes standards** : autres systèmes d'information et de communication et les services numériques non caractérisés comme essentiels ou importants.

ANNEXE 23

LE DOSSIER DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (DSSI)

Le dossier de sécurité d'un système d'information (DSSI) classifié contient les informations nécessaires pour évaluer la sécurité dans le cadre d'une inspection, d'un contrôle, d'un audit, d'un avis technique d'aptitude informatique (ATAI) ou d'une intervention de l'État dans le cadre d'un incident.

Le modèle de dossier de sécurité d'un système d'information est fourni par le service enquêteur et peut évoluer en fonction du contexte, de la société et des systèmes d'information mis en œuvre. Ainsi, les informations utiles à la compréhension du système numérique et de son environnement peuvent être ajustées, autant que de besoin.

De manière générique, le dossier de sécurité d'un système d'information vise à décrire les éléments suivants :

- la **présentation de la société** et de l'établissement concerné ;
- la **description du système numérique** et notamment :
 - o la cartographie détaillée du système, conformément à la fiche 6.1 de la présente instruction ;
 - o les procédures d'exploitation de la sécurité et les éventuelles politiques définies et mises en œuvre par l'entité sur le système numérique considéré, permettant de contrôler la conformité de l'implémentation avec les mesures décrites ;
 - o tout élément permettant d'attester que les constituants physiques du système numérique sont situés dans des locaux aptes à traiter des informations du niveau requis et que, le cas échéant, les liens informatiques cheminant hors de ces locaux sont conformes aux dispositions de la fiche 6.10 de la présente instruction (exemples : référence de l'avis technique d'aptitude physique plan de masse, plan des circuits approuvés, etc.) ;
 - o tout élément permettant d'assurer que les mesures de protection contre les signaux parasites compromettants sont conformes aux réglementations applicables (exemples : détail des mesures mises en œuvre, références des résultats de mesures d'atténuation électromagnétique (Tempest) réalisées par un organisme accrédité, etc.) ;
 - o tout élément permettant d'assurer que les supports numériques classifiés sont gérés conformément à la présente instruction (exemples : extrait de l'inventaire des informations et supports classifiés, détail des procédures de gestion, etc.) ;
- les **informations relatives aux acteurs internes et externes intervenant sur le système numérique**, notamment tout élément permettant d'établir que les personnes ayant accès au système numérique ou à ses constituants physiques sont habilitées au niveau attendu (exemples : liste des personnes accédant aux informations et supports classifiés, listes des sous-traitants, etc.).

Pour rappel, toute déclaration fausse ou inexacte donnée sciemment à une administration est susceptible d'engager la responsabilité pénale de l'entité (article 441-1 du code pénal).