



CEA/DAM/DCG/SAP
DO 55 20/03/23



diffusé le : 21/03/23

**Dispositions applicables aux Titulaires de marchés
passés par le CEA/DAM concernant les
informations protégées par la mention
*Diffusion Restreinte***
—
Déclinaison en règles de sécurité informatique

SYM S02XX SJD DIR 23000188 B

TABLEAU DES EVOLUTIONS

Edition	Motif et nature des évolutions	Date
Indice A	Edition initiale	15/12/2014
Indice B	Prise en compte de la nouvelle IGI 1300 (arrêté du 9 août 2021)	19/01/2023

SOMMAIRE

Objet	4
Documents de référence	4
Chapitre 1 : Principes de sécurité des systèmes d'information - Conditions d'usage	5
1 Nature des marchés impliquant la détention d'informations classifiées ou sensibles	5
2 Le classement des informations	5
3 Principes de sécurité des SI pour les marchés classifiés ou sensibles (informations protégées DR)	6
3.1 – Cas du traitement, sur le SI de l'entreprise titulaire du Marché, d'informations ou supports classifiés de niveau Secret ou Très Secret	6
3.2 – Cas du traitement par le Titulaire d'informations ou supports sensibles non classifiés, identifiés par la mention Diffusion Restreinte	6
4 Les échanges d'informations entre le Titulaire et le CEA/DAM	7
5 Synthèse des principes applicables	9
Chapitre 2 : Prescriptions de sécurité des systèmes d'information sensibles	10
1 Objet	10
2 Terminologie	10
3 Documents de référence	10
4 Intervenants & fonctions	10
5 Domaine d'application – Obligation de transfert.....	10
6 Réseau informatique spécifique	10
6.1 – Réseau spécifique Diffusion Restreinte	12
6.2 – Réseau spécifique classifié de défense (cas exceptionnel).....	12
7 Les systèmes industriels	12
8 Gestion des supports amovibles	14
9 Gestion des comptes.....	14
10 Sauvegardes.....	15
11 Audits du CEA	15
Chapitre 3 : Prescriptions pour les échanges d'informations sensibles non classifiées	16
1 Objet	16
2 Terminologie.....	16
3 Echanges avec le CEA/DAM.....	16
3.1 – Messagerie électronique	16
3.2 – Réunions	16
3.3 – Intervention sur Centre CEA/DAM	16
4 Logiciels de chiffrement de conteneur.....	17
5 Audits du CEA	17
Annexe 1 - Glossaire	18
Annexe 2 - Guide d'utilisation de la version Zed Limited Edition à date	19

Objet

Le présent document a pour objet de définir les prescriptions de sécurité informatique de la Direction des applications militaires du Commissariat à l'énergie atomique et des énergies alternatives (CEA/DAM) pour les systèmes d'informations (SI) traitant des informations sensibles non classifiées de défense à destination des Titulaires de marchés où le CEA/DAM est pouvoir adjudicateur. Il complète les conditions générales d'achat (CGA) du CEA dans leur version applicable.

Il se décompose en trois chapitres et deux annexes :

1. Un premier chapitre didactique ayant pour vocation de rappeler les grands principes qui permettent au Titulaire d'un marché du CEA/DAM de comprendre clairement le contexte du marché et les obligations afférentes en matière de Sécurité des Systèmes d'Information (SSI) ;
2. Un deuxième chapitre qui définit les prescriptions de sécurité informatique du CEA/DAM pour les SI du Titulaire devant, le cas échéant, accueillir des données protégées par la mention *Diffusion Restreinte* ;
3. Un troisième chapitre qui définit les prescriptions de sécurité informatique pour les échanges d'informations protégées par la mention *Diffusion Restreinte* entre le CEA/DAM et le Titulaire ou avec ses éventuels sous-traitants ou cotraitants ;
4. Deux annexes : glossaire et Guide d'utilisation de la version Zed Limited Edition à date.

Ces chapitres, et notamment les chapitres 2 et 3, sont autoporteurs et peuvent être utilisés indépendamment les uns des autres.

Documents de référence

Dans leur version applicable :

- IGI 1300 Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale
- IM 900 Instruction ministérielle n°900 sur la protection du secret et des informations *Diffusion Restreinte* et sensibles
- II 901 Instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles

Guides de l'ANSSI¹ :

- Guide d'Hygiène Informatique
- L'homologation de sécurité en neuf étapes simples
- Recommandation pour les architectures des systèmes d'information sensibles ou diffusion restreinte
- Recommandations relatives à l'interconnexion d'un système d'information à Internet
- Guide « Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information »
- Guide d'élaboration de politiques de sécurité des systèmes d'information
- Maîtriser la SSI pour les systèmes industriels

¹ Disponibles sur le site de l'ANSSI (<https://www.ssi.gouv.fr>), catégorie 'UNE ENTREPRISE'

Chapitre 1 : Principes de sécurité des systèmes d'information - Conditions d'usage

1 Nature des marchés impliquant la détention d'informations classifiées ou sensibles

Les marchés pouvant mettre en œuvre des informations classifiées ou sensibles passés par le CEA/DAM sont qualifiés :

- de Marché classifié avec détention d'informations ou supports classifiés (ci-après dénommés « ISC ») lorsque le Titulaire a accès à des informations ou supports classifiés dans ses locaux ou dans des locaux mis à sa disposition par le CEA/DAM ;
- de Marché classifié avec accès à (sans détention) des ISC lorsque le Titulaire a accès à des informations ou supports classifiés dans les locaux du CEA/DAM sans détention de ces ISC ;
- de Marché sensible lorsque le marché est exécuté par le Titulaire dans des lieux abritant des ISC ;
- de Marché dans le cadre duquel le Titulaire a accès à (et peut détenir) des informations ou supports protégés par la mention *Diffusion Restreinte* (DR)², y compris éventuellement avec la mention complémentaire de protection *Spécial France*³ ;
- de Marché sans mention de protection dans les autres cas.

En application des dispositions de l'IGI 1300, les marchés qui le nécessitent intègrent les clauses adéquates de protection du secret ou de confidentialité et, le cas échéant, font l'objet d'un Plan contractuel de sécurité (PCS).

Toutes les dispositions en matière de protection de l'information DR applicables au Titulaire d'un tel marché sont applicables à ses sous-traitants dans le cadre de l'exécution dudit marché dans la mesure où les prestations sous-traitées traitent de l'information protégés par la mention DR.

2 Le classement des informations

Le CEA/DAM applique les définitions réglementaires nationales relatives à la protection de l'information, par sensibilité décroissante :

- les **informations classifiées** : *Très Secret* (anciennement *Secret Défense*) ou *Secret* (anciennement *Confidentiel Défense*).
- les **informations sensibles**, non classifiées, dont la divulgation est susceptible d'induire une perte, une nuisance ou une gêne au CEA/DAM ; elles portent une mention : en général *Diffusion Restreinte* (DR), voire DR - *Spécial France*.
- les **informations de Diffusion Ordinaire** (DO), destinées à une diffusion large sans jamais être publique. Elles peuvent prendre le statut d'information ouverte après autorisation de publication. Elles ne portent pas de mention.

Il est du ressort exclusif de l'unité prescriptrice du CEA/DAM d'identifier et de définir le périmètre des informations ou supports sensibles non classifiés (DR) qui sont transmis au Titulaire. Les informations ou supports correspondant portent la mention *Diffusion Restreinte*.

² Marché qui ne peut pas être qualifié de « Marché sensible » car il ne s'exécute pas dans des lieux abritant des ISC.

³ La mention complémentaire *Spécial France* impose au Titulaire de limiter l'accès des données du Marché aux seuls ressortissants français et d'interdire l'accès de ces mêmes données à des personnes morales de droit étranger (IGI 1300)

3 Principes de sécurité des SI pour les marchés classifiés ou sensibles (informations protégées DR)

Du point de vue des SI du Titulaire, les contraintes de sécurité ne sont liées qu'aux informations détenues par celui-ci.

Les dispositions relatives à la protection de l'information DR doivent être appliquées aux marchés qualifiés de « Marché classifié avec accès à (sans détention) des ISC » qui mettent en œuvre uniquement des données sensibles non classifiées de défense sur le SI du Titulaire. Il en va de même pour les « Marchés sensibles » et pour les Marchés dans le cadre desquels le Titulaire aura accès ou aura à détenir des informations ou supports DR.

3.1 – Cas du traitement, sur le SI de l'entreprise titulaire du Marché, d'informations ou supports classifiés de niveau Secret ou Très Secret

Le Marché établi avec l'entreprise est un contrat classifié du niveau de confidentialité adapté avec détention d'ISC. La responsabilité du Titulaire de respecter les obligations portées par l'IGI 1300, l'II 901 et l'IM 900 lui est propre. Le Titulaire fait intervenir des personnels habilités et fera valoir, sinon fait procéder, à l'homologation du SI concerné. Pour cela, il dispose de locaux dont une aptitude physique aura été délivrée par le service enquêteur compétent. Aucune exigence complémentaire n'est demandée par le CEA/DAM sur le SI homologué. La présentation par le Titulaire au CEA des attestations d'aptitude physique des locaux et du procès-verbal (PV) d'homologation des SI est un préalable à la signature du Marché.

3.2 – Cas du traitement par le Titulaire d'informations ou supports sensibles non classifiés, identifiés par la mention Diffusion Restreinte

Si le Marché établi avec l'entreprise est un marché classifié avec accès (sans détention), ou un marché sensible, ou un marché dans le cadre duquel le Titulaire aura accès ou détient des informations ou supports DR, l'exécution du Marché implique le traitement d'informations ou supports sensibles (DR) par le Titulaire.

Les prescriptions de sécurité relatives aux SI abritant des données sensibles non classifiées (voir chapitre 2) sont applicables.

Les exigences réglementaires sont les suivantes :

Le Titulaire s'engage à traiter ces informations ou supports, portant la mention de protection DR, dans le respect des règles édictées par les dispositions légales et réglementaires en vigueur : IGI 1300, II 901, IM 900 ainsi que les guides de l'ANSSI listés dans les documents de référence cités page 4. La responsabilité de l'entreprise de respecter les obligations exprimées par ces règles, et notamment celles de l'II 901 pour son SI, lui est propre. Les points les plus importantes de ces règles sont synthétisées par ce qui suit.

Les SI aptes à traiter des informations DR doivent faire l'objet d'une homologation de sécurité (annexe 1, § 5 de l'IGI 1300). En conséquence, les SI utilisés par le Titulaire et ses éventuels cotraitants et sous-traitants pour traiter et élaborer les documents DR dans le cadre de l'exécution du marché doivent être :

- des SI homologués par l'Autorité Qualifiée de l'entreprise, aptes à traiter des informations classifiées ; ou
- des SI homologués par l'Autorité Qualifiée de l'entreprise, aptes à traiter des informations DR.

En général, conséquence du principe du besoin d'en connaître, le Titulaire est amené à dédier un SI à l'exécution du Marché. Pour le traitement des informations DR, l'II 901 exige alors que le réseau de ce SI soit :

- de classe 1 (communicant avec Internet par une passerelle filtrante dotée d'un dispositif de traçabilité et d'alerte, de surcroît qualifiée par l'ANSSI ou un organisme agréé) ou
- de classe 2 (isolé d'Internet).

La difficulté de se prémunir des risques issus d'Internet et l'indisponibilité à court ou moyen terme de solutions de classe 1, amène le CEA/DAM à exiger que le réseau de ce SI soit de classe 2, isolé, c'est-à-dire non connecté, même indirectement à Internet (annexe 2 de l'II 901).

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

Dans la mesure où le Titulaire ne dispose pas d'un SI conforme aux exigences de l'II 901 pour le traitement des informations DR, le CEA/DAM peut accepter certaines dispositions pratiques et préconiser des solutions pragmatiques issues de l'II 901. Ces dispositions ou solutions ne peuvent être appliquées qu'après accord écrit du CEA/DAM.

Dans le cas d'entreprises possédant un SI adapté à la protection de l'information DR, il est possible que la sécurité soit conforme aux objectifs d'un réseau de classe 1 : dans ce cas, le Titulaire fournit la description précise du SI et des conditions de traitement sur ce réseau des informations ou supports DR du Marché. Dans le cas d'un SI homologué, le Titulaire fournira son PV d'homologation au CEA/DAM.

Dans le cas où le Titulaire ne manipule que très peu d'informations DR au sens défini au §2 de ce chapitre, des solutions pragmatiques et de compromis qui maintiennent l'isolement de ces informations d'Internet peuvent être prises sous réserve de l'accord préalable du CEA/DAM. Elles ne peuvent être appliquées qu'après accord écrit du CEA/DAM.

A titre d'exemple de solution pragmatique pour la gestion de l'information DR : dans l'attente d'une homologation, des SI constitués d'un ordinateur ou d'un réseau qui obéissent aux règles suivantes :

- le système est dédié aux applications bureautiques propres à l'entreprise ;
- le système ne possède aucune connexion avec Internet⁴ ;

pourront être utilisés.

Dans tous les cas, le Titulaire devra confier l'administration de ces SI à des administrateurs respectant les règles élémentaires d'hygiène informatique définies par l'ANSSI et celles de ce chapitre. Tout administrateur d'un SI *Diffusion Restreinte* doit de plus être habilité au niveau Secret.

Enfin, il est des informations, en général créées par le Titulaire, qui ne bénéficient pas de mention de protection pour des raisons techniques (codes automate, fichiers techniques ou de paramétrage, etc.). De même que précédemment, le Titulaire y applique des règles de protection adaptées prises en accord avec le CEA/DAM.

4 Les échanges d'informations entre le Titulaire et le CEA/DAM

L'exécution du Marché implique des échanges d'informations entre le Titulaire du Marché et le CEA/DAM. *Attention, en cas d'échange d'informations ou supports classifiés le Titulaire doit respecter les règles d'acheminement, marquage et traçabilité prescrites par l'IGI 1300. L'échange de documents électroniques ne peut se faire que sur des supports classifiés dûment enregistrés ou éventuellement via des supports agréés.*

Néanmoins, le suivi régulier du Marché peut impliquer l'échange d'informations ou supports non classifiés, et ce indépendamment de la classification générale du marché.

Sous réserve que le cumul des informations échangées au cours du temps ne relève pas de l'information classifiée, il est possible d'échanger de l'information DR en conteneur chiffré dans des conditions conformes à l'II 901 (il en va de même pour les marchés sensibles et les marchés dans le cadre duquel le Titulaire a accès à et peut détenir des informations ou supports DR). Pour cela, le CEA/DAM exige l'utilisation de solutions de conteneurs chiffrés agréés par l'ANSSI dans le respect des conditions d'emploi de l'agrément.

Parmi les solutions agréées par l'ANSSI pour le transport de données sensibles, le CEA/DAM en a déployé deux sur ses postes de travail : ACID Cryptofiler et ZoneCentral et ses conteneurs associés Zed. Pour les échanges avec le CEA/DAM, le choix de la solution sera nécessairement entre ces deux possibilités. Pour les besoins propres du Titulaire, le choix de la solution devra se faire prioritairement entre ces deux possibilités, en concertation avec le CEA. L'adoption de toute autre solution agréée ANSSI nécessite un accord préalable écrit du CEA/DAM.

⁴ Filiale, Wi-Fi, GSM, etc.

PRINCIPES GENERAUX

Le Titulaire s'engage à appliquer les règles suivantes pour toute communication d'informations DR par voie électronique réalisée dans le cadre du Marché (et notamment toute communication entre les membres de son personnel, avec ses cotraitants et sous-traitants ou avec le CEA/DAM).

1. Aucun message de niveau DR (corps du message et pièce jointe) n'est transmis en clair sur Internet.
2. Tout document de niveau DR doit être transmis dans des conteneurs chiffrés suivant les dispositions des paragraphes ci-après.

MANIPULATION DES CONTENEURS CHIFFRES

Le Titulaire disposant préalablement du logiciel de chiffrement ACID Cryptofiler peut échanger avec le CEA par ce moyen. Pour ce faire, les clés publiques ACID des correspondants peuvent être échangées sur l'Internet.

A défaut, le logiciel de chiffrement ZoneCentral ou Zed est utilisé. Pour ce faire, un conteneur Zed vide peut être mis à disposition du Titulaire par le CEA. Le mot de passe d'accès est transmis aux personnes concernées par une voie spécifique (courrier, téléphone). Le mot de passe, qu'il est conseillé de noter dans un document protégé de niveau DR, n'est écrit sur aucun système informatique. Les conteneurs Zed doivent être utilisés uniquement à l'aide du logiciel ZoneCentral ou la version qualifiée gratuite du logiciel Zed⁵ disponible sur le site de l'éditeur Prim'x :

(<https://client.primx.eu/PublicSoftware/zedlimitededition/>).

Le fichier xxx_DR.zed pourra être décrypté à l'aide du logiciel téléchargeable à l'adresse ci-dessus. Un guide d'utilisation de cette version à date est disponible en annexe 2.

Les conteneurs chiffrés, Zed ou ACID, sont transférés sur le SI sécurisé du Titulaire. Symétriquement, les documents à expédier sont mis en conteneur sur le SI sécurisé, avant toute expédition en pièce jointe de messagerie.

POLITIQUE DES MOTS DE PASSE

Les règles minimales pour la composition des mots de passe sont décrites ci-après.

- Longueur minimale : de niveau de sensibilité moyen à fort (au sens de l'ANSSI), soit 12 caractères à date ;
- Composition : nombre de jeux de caractères différents = 3 ;
- Durée de vie : le temps de l'exécution du Marché.

EXIGENCES DE COMPOSITION

- Ne pas contenir 5 caractères consécutifs du nom, prénom, numéro de badge du salarié ou dernier mot de passe ;
- Ne pas contenir un mot issu d'un dictionnaire (français, anglais) ni, autant que possible, des combinaisons triviales (1234, azerty, etc.) ;
- Ne pas contenir plus de 2 fois consécutives le même symbole.

⁵ A date, la version Q.2020.1 pour Windows certifiée le 22/08/2022

5 Synthèse des principes applicables

Le tableau ci-dessous synthétise pour les différentes natures d'informations les règles applicables en termes de gestion sur le SI du Titulaire ou d'échange avec ses sous-traitants ou avec le CEA/DAM.

	Nature des informations		
	Secret / Très Secret (CD/SD)	<i>Diffusion Restreinte</i>	Diffusion Ordinaire
SI du Titulaire	Selon IGI 1300	Chapitre 2 ^(*)	Pas de dispositions particulières
Échange électronique des informations	Interdit entre SI de classification différentes et entre SI classifié et non classifié	Chapitre 3 ^(*)	Pas de dispositions particulières

(*) Dans la mesure où l'exécution du marché ne met en œuvre que quelques informations sensibles non classifiées et sur décision préalable écrite du CEA/DAM, les dispositions minimales suivantes peuvent être appliquées :

- Sur le SI du Titulaire, les données sont stockées sous forme chiffrée. Elles ne sont manipulées en clair que lorsque le SI est déconnecté physiquement d'Internet.
- Les échanges d'informations sensibles sont réalisés sous forme chiffrée dans les conditions prescrites par ce document.

Documents de référence (dans leur version applicable) : voir liste en page 4.

Chapitre 2 :

Prescriptions de sécurité des systèmes d'information sensibles

1 Objet

Le présent chapitre précise les exigences du CEA/DAM liées à la sécurité informatique dans ses projets/marchés réalisés avec des partenaires industriels. Il précise les dispositions nécessaires à la protection des informations *Diffusion Restreinte* en application de l'IGI 1300, de l'IM 900 et de l'II 901. Il vient en application des obligations déclinées dans le Plan Contractuel de Sécurité (PCS) du marché, qui définit le niveau de classification ou, le cas échéant, de protection du marché et la sensibilité de ses composantes informationnelles.

2 Terminologie

Le glossaire est joint en annexe 1 des présentes dispositions.

3 Documents de référence

Dans leur version applicable, voir liste en page 4.

4 Intervenants & fonctions

Le Titulaire désignera officiellement, au plus tard à la réunion de lancement ou d'enclenchement du Marché, un RSSI (Responsable de la sécurité des systèmes d'information) pour les aspects SSI. Lors du début de l'exécution du Marché, le Titulaire désignera un responsable d'exploitation du ou des SI concernés de l'entreprise. Dans tous les cas, le Titulaire s'engage à confier l'administration des SI concernés à des administrateurs comme précisé au chapitre 1 §3.2.

Le CEA/DAM indiquera l'OSSI (Officier de sécurité des systèmes d'information) du centre ainsi que, si nécessaire, le RSSI en charge de l'installation ou du projet désigné pour encadrer l'application des prescriptions de SSI. Cet OSSI de centre est à même de prescrire d'éventuelles dispositions particulières ; pour la délivrance de certificats nécessaires aux systèmes de chiffrement, il est autorité de certification du centre.

5 Domaine d'application – Obligation de transfert

Ces dispositions s'appliquent aux informations sensibles telles que définies au chapitre 1. Elles s'appliquent au Titulaire ainsi qu'à l'ensemble de son personnel amené à travailler dans le cadre du Marché. Si le Titulaire a recours à des sous-traitants, il s'oblige à transférer l'ensemble des présentes dispositions à ses sous-traitants dans la mesure où ceux-ci ont besoin d'avoir accès et/ou de détenir des informations ou supports sensibles.

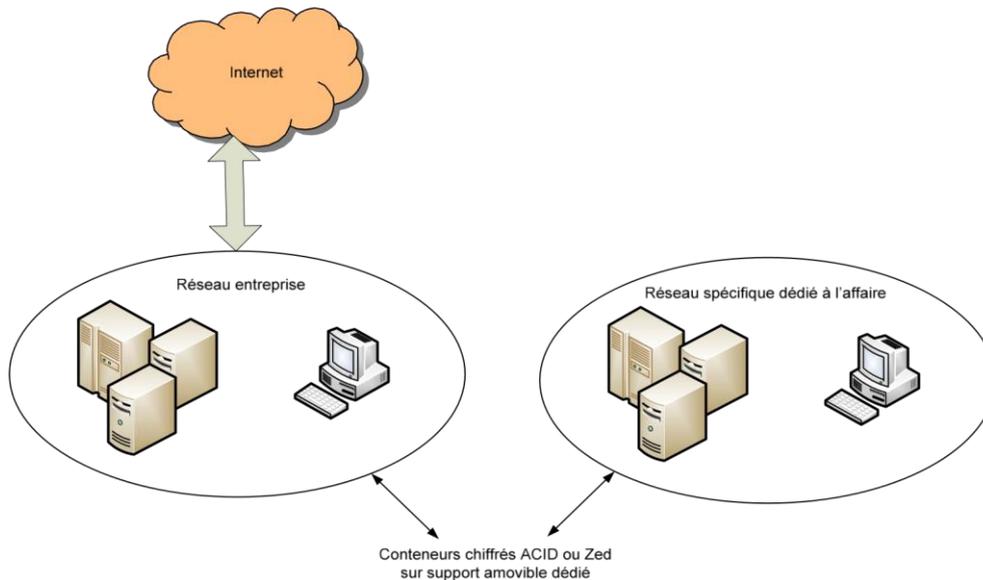
6 Réseau informatique spécifique

Dans le cas où le Titulaire possède un réseau d'entreprise qui lui est propre et qui est conforme aux exigences de l'IM 900, l'II 901 et de l'IGI 1300 pour le traitement des informations *Diffusion Restreinte*, les exigences de ce paragraphe 6 ne s'appliquent pas, notamment l'isolement d'Internet. Le Titulaire fournira le procès-verbal d'homologation de ce réseau et des conditions de traitement, sur celui-ci, des informations sensibles qui font l'objet du Marché. Ces éléments sont à fournir au CEA de manière préliminaire dans l'offre du Candidat/Soumissionnaire puis de manière définitive dans ou en accompagnement des documents de gestion de projet (Plan d'Assurance Qualité, Plan de Management, ...) et le cas échéant dans le PCS.

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

Pour les autres réseaux spécifiques qui seraient destinés au traitement des informations DR dans le cadre du Marché, il est convenu, entre le CEA/DAM et le Titulaire, qu'aucun fichier sensible relatif à l'exécution du Marché ne sera implanté sur une machine (serveur, ordinateur portable, ordinateur individuel, PDA...) directement connectée avec Internet et ce, quelle que soit la connexion (filaire, Wi-Fi, GSM...). De ce fait, l'intégralité des fichiers correspondants sera implantée sur un système⁶ physiquement déconnecté d'Internet (directement et indirectement). Par la suite, ce SI dédié⁷ à l'affaire sera dénommé « réseau spécifique ».

Le schéma ci-dessous représente la configuration autorisée par le CEA/DAM :



Le réseau spécifique du Titulaire est a minima de niveau *Diffusion Restreinte*, mais il est possible que, dans des cas exceptionnels, le Titulaire utilise un réseau classifié de défense qui lui est propre.

Quel que soit son statut, et en complément des dispositions réglementaires applicables (IGI 1300, II 901, IM 900) et des guides de l'ANSSI, le réseau spécifique doit notamment obéir aux principales dispositions réglementaires suivantes :

- Toute connexion directe ou indirecte du réseau spécifique avec Internet est strictement interdite.
- Toute connexion directe ou indirecte d'une ou plusieurs des stations de travail du réseau spécifique avec Internet est strictement interdite.
- Les technologies de transmission sans fil sont interdites, de ce fait le réseau spécifique est constitué uniquement de liaisons filaires.
- Toute connexion d'un téléphone portable au réseau spécifique est interdite ; le raccordement d'équipements mobiles particuliers nécessaires à l'exécution du marché doit préalablement faire l'objet d'une analyse de sécurité.
- Le réseau spécifique doit être protégé par un antivirus et un anti-malware mis à jour régulièrement, au minimum de manière hebdomadaire.
- Une traçabilité des connexions, déconnexions (réussies et en échec) est mise en place, couvrant la durée de vie du système. Les traces système seront paramétrées (localement sur les postes de travail et/ou sur serveur d'authentification s'il y en a un) pour couvrir cette durée. L'intégrité des traces est confiée à la responsabilité de l'administrateur local.

⁶ Dans certains cas, il peut s'agir d'une machine unique.

⁷ Le réseau peut être utilisé pour d'autres affaires du CEA, sous réserve d'accord du CEA/DAM et des responsables CEA des affaires concernées.

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

L'utilisation de SI mobiles (téléphone portable, smartphone, etc..) présente des risques (communication sans fil, capacité de stockage et traitement d'information, prises de vue), il revient au RSSI du Titulaire de sensibiliser ses utilisateurs, voire de mettre à disposition des consignes pour déposer ces appareils en dehors de la zone de travail du réseau spécifique.

6.1 – Réseau spécifique *Diffusion Restreinte*

Pour la gestion d'informations ou supports sensibles non classifiés de défense (DR maximum), le Titulaire (personne morale) et son personnel participant à l'exécution du Marché (y compris les administrateurs de ces SI spécifiques) peuvent faire l'objet d'une enquête administrative à la demande du CEA/DAM. Les administrateurs des SI *Diffusion Restreinte* doivent être habilités au niveau **Secret**.

Le Titulaire met en place un réseau informatique spécifique DR.

Il est convenu entre les Parties que le Titulaire est en charge dès le début de l'exécution du Marché de la conception, la fourniture et la mise en place du réseau spécifique, que cela concerne le software, le hardware, tous les périphériques (tels qu'imprimantes, traceurs, scanner, lecteurs divers, baies de brassage, switch, câbles, écrans...). Les conditions de réutilisation d'un SI préexistant sont soumises à la validation du CEA/DAM.

Le Titulaire est par ailleurs averti que l'intégralité des mémoires rémanentes qui auront été connectées au réseau spécifique (serveurs, stations de travail, imprimantes...) devra être remise au CEA/DAM en fin d'exécution du Marché. Dans certains cas, une attestation sur l'honneur d'effacement sécurisé des données de l'affaire peut être acceptée après accord du CEA sur la procédure d'effacement. La date de fin d'exécution du Marché est définie par le responsable CEA du contrat, en général quand les obligations de garantie ou de maintenance n'imposent pas au Titulaire une obligation de conservation des informations.

Une description conforme de l'organisation du réseau spécifique et la liste des serveurs, postes informatiques sur lesquels seront implantés les documents du projet et le logiciel de chiffrement sera remise par le Titulaire au démarrage de l'exécution du Marché et au plus tard à la réunion d'enclenchement/lancement. Le document est mis à jour lors de toute évolution significative du système (évolution matérielle ou changement dans les principes d'exploitation).

6.2 – Réseau spécifique classifié de défense (cas exceptionnel)

Pour l'exploitation et l'utilisation de ce SI classifié de défense (S (ex CD) ou TS (ex SD)), et conformément à l'IGI 1300, le Titulaire fait intervenir des personnels habilités, dispose de locaux dont une aptitude physique aura été délivrée par l'autorité compétente, et le SI aura fait l'objet d'une homologation.

Le réseau spécifique utilisé dans le cadre de l'exécution du Marché pourra être le réseau classifié du Titulaire suivant un accord explicite préalable du CEA/DAM. Dans ce cas, le Titulaire s'organisera pour regrouper les données liées au marché afin de pouvoir s'engager à les détruire⁸ en fin d'exécution, sur demande explicite du responsable CEA/DAM du Marché et de respecter le besoin d'en connaître au sein du personnel du Titulaire. Dans tout autre cas, les exigences du paragraphe 6.1 sont applicables.

7 Les systèmes industriels

Les systèmes industriels (automates programmables industriels, déports d'entrées et sorties, réseaux de terrain, etc.) sont exposés à des risques de malveillance, à plus forte raison s'ils sont déployés sur des installations sensibles.

⁸ La procédure d'effacement sécurisé ainsi que les éventuels résidus dans les systèmes de sauvegarde sont soumis à l'acceptation du CEA.

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

Dans le cadre de ses prestations, pendant les phases de conception, d'intégration et de maintenance des systèmes industriels, le Titulaire doit mettre en œuvre les bonnes pratiques des guides de l'ANSSI⁹ qui sont rappelées, sans être exhaustives (référence des bonnes pratiques associées), ci-dessous :

- BP01 : Contrôle d'accès physique aux équipements
 - o maîtriser les points d'accès physique qui permettraient de s'introduire dans le système. Les équipements concernés sont les serveurs, postes opérateurs, équipements réseau, automates, capteurs/actionneurs, écrans tactiles ;
- BP02 : Cloisonnement des réseaux
 - o les développements doivent se faire sur le réseau spécifique ;
 - o le raccordement d'une machine (PC portable de maintenance) non dédiée à l'exécution du marché (ou au CEA/DAM) est à proscrire. En cas de nécessité incontournable, les conditions d'utilisation d'un PC mutualisé sont précisées et préalablement validées par le CEA/DAM ;
 - o séparer les flux réseaux par des équipements dédiés ou des VLAN (virtual local area network) ;
- BP03 : Gestion des médias amovibles
 - o réduire les risques liés à l'utilisation de médias amovibles ;
 - o installer des machines dédiées aux transferts de données, désactiver les ports USB sur les systèmes, définir une politique d'utilisation des médias amovibles ;
- BP04 : Gestion des comptes
 - o définir une politique de gestion des comptes utilisateurs et des comptes d'application. Ne pas laisser de compte par défaut (admin/admin par exemple), ne pas utiliser de compte générique, définir une robustesse et durée de vie des mots de passe éventuellement en accord avec les règles du CEA/DAM ;
- BP05 : Durcissement des configurations
 - o n'installer que les logiciels, protocoles et services nécessaires. Désactiver les modes de configuration et de programmation à distance ;
 - o s'assurer que les versions actives dans les équipements (version N) n'ont pas été modifiées, identifier et analyser les écarts des versions N et N-1 avant la mise en service de nouvelles versions ;
- BP06 : Gestion des journaux d'évènements et d'alarmes
 - o tracer les actions et les interventions de maintenance (journaux d'évènements et d'alarmes) afin de permettre de détecter des intrusions ;
- BP08 : Sauvegardes / restaurations
 - o définir et mettre en œuvre une politique de sauvegarde des données¹⁰ (y compris les données des systèmes) ;
- BP09 : Documentation
 - o maîtriser la documentation pour disposer d'une image exacte des installations et maîtriser sa diffusion pour gérer le besoin d'en connaître ;
 - o maintenir à jour (et fournir à la livraison) le dossier du système : cartographie physique et réseau adressé, descriptif système, dossiers de fichiers et programmes applicatifs, liste des comptes, des services, des protocoles, des temps caractéristiques ;
- BP10 : Protection antivirale
 - o protéger les équipements et applications contre les virus et malware. Définir et mettre en œuvre une politique antivirale ;

⁹ Se référer aux guides de l'ANSSI (documents de référence).

¹⁰ Il peut s'agir par exemple des codes sources des applications, des bases de données, des journaux de supervision, des programmes des automates, des fichiers de configuration des équipements réseau, etc.

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

- BP11 : Mise à jour des correctifs
 - définir et mettre en œuvre une politique de gestion des correctifs des systèmes d'exploitation, des applications, des micrologiciels (firmwares) : systématique, périodique ou ponctuelle, adaptée aux contraintes fonctionnelles et aux risques identifiés ;
- BP12 : Protection des automates
 - sécuriser l'accès aux automates. Les équipements sont dans des baies fermées à clef, les accès au code source et au code embarqué dans les automates sont protégés ;
 - sécuriser les postes de développement et les consoles de programmation automates. Appliquer les correctifs, activer un antivirus. Dédier les machines au système concerné et tracer leur utilisation – à défaut, expliciter les conditions de mutualisation avec d'autres affaires ou projets.

8 Gestion des supports amovibles

Dans le cadre de l'exécution du Marché, il s'agit de clés USB¹¹, de CD-ROM ou de disques amovibles, a minima de niveau DR, à l'exception des systèmes de stockages réseau (type rack, baies ou armoires de disques, NAS,...). Tous ces supports sont neufs, distincts des autres affaires et acceptés par le CEA/DAM avant usage. L'utilisation des supports amovibles DR est autorisée suivant les conditions suivantes :

- les supports sont parfaitement identifiés et tracés dans un registre ;
- ils sont dédiés à l'affaire en cours ;
- l'utilisation de clés USB ne sert qu'à faire du transfert de fichiers DR chiffrés entre le réseau spécifique et le CEA via internet ;
- les clés USB ne sont pas utilisées pour faire du stockage ou de l'archivage de données ;
- tous les fichiers de l'affaire contenant des informations sensibles, déposés sur ces supports, sont chiffrés avec le logiciel de chiffrement ACID ou ZoneCentral ;
- il est toléré que des fichiers non sensibles (DO), tels que des fichiers constructeurs, soient non chiffrés ;
- il est recommandé de procéder régulièrement à un effacement sécurisé¹² des clés USB (par exemple, avec l'exécutable cipher fourni avec Windows) ;
- à la fin de la prestation et au plus tard à la fin des obligations du Titulaire, la totalité des supports amovibles est remise au CEA/DAM (à l'exception des systèmes de stockage réseau ci-dessus), un procès-verbal sera alors adressé au RSSI de l'installation ou du projet désigné ;
- l'utilisation de tout autre support amovible sur un poste informatique du réseau spécifique est strictement interdite.

La copie d'un fichier sensible lié à l'exécution du Marché sur un support amovible ne s'effectuera qu'après son chiffrement par ACID Cryptofiler ou Zed. Aucun fichier sensible non chiffré ne devra être placé sur un support amovible.

En fin d'exécution du marché, les supports amovibles devenus inutiles ou périmés, seront détruits par le CEA/DAM ou le Titulaire selon les recommandations de l'IGI 1300 et suivant la décision préalable du CEA/DAM. Un procès-verbal de destruction sera dressé par le responsable de la destruction et transmis à l'autre Partie. Pour les systèmes de stockage réseau ci-dessus, une attestation sur l'honneur de destruction sécurisée de toutes les données DR par le Titulaire sera communiquée au CEA/DAM.

9 Gestion des comptes

Le RSSI du Titulaire assure que l'administration du SI est conforme aux bonnes pratiques de sécurité. A ce titre, il est notamment responsable de la gestion des comptes informatiques créés pour l'accès aux SI ou réseaux spécifiques.

¹¹ Les clés USB peuvent être interdites sur certains systèmes du CEA

¹² Pour réellement supprimer les fichiers, il faut réécrire des données sur l'espace mémoire ou disque qu'ils occupaient, par « surcharge » de cet espace.

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

En particulier, toute action sur le SI doit pouvoir être imputée à une personne. L'ouverture d'une session sur un réseau spécifique est donc impérativement nominative.

Les utilisateurs standards du SI ne doivent pas être en mesure de mettre en défaut l'intégrité système du SI ; ils ne doivent donc posséder aucun privilège administrateur.

Le RSSI du Titulaire tient à jour un registre listant les utilisateurs du SI, leurs profils d'accès (utilisateur standard, administrateur système, maintenancier...) et la justification du besoin d'accès privilégiés.

Au cas où le réseau spécifique se résume à une unique machine, le CEA/DAM préconise :

- que le système et les données soient placés dans deux partitions distinctes,
- que les utilisateurs standards ne puissent pas modifier le système,
- que les données ne soient accessibles qu'aux seuls utilisateurs autorisés.

10 Sauvegardes

Les Parties conviennent que, dans le cas d'un système dédié à la réalisation du Marché, une sauvegarde des données sera réalisée par le Titulaire et sous sa responsabilité. Le support de sauvegarde pourra être :

- des CD ROM ou DVD ROM, qui devront alors être stockés dans une armoire fermée à clés.
- des disques durs amovibles, qui devront alors être stockés dans une armoire fermée à clés.
- une ou plusieurs machines du réseau spécifique.

Les supports utilisés pour les sauvegardes sont identifiés et tracés dans un registre. Les supports de sauvegarde devront être remis au CEA/DAM en fin d'affaire, au terme de l'exécution du marché.

Pour les sauvegardes réalisées sur des systèmes de stockage réseau tels que défini au §8, des Plans de sauvegarde spécifiques au Marché sont mis en place avec l'accord du CEA/DAM, une attestation sur l'honneur de destruction sécurisée de toutes les données DR par le Titulaire sera communiquée au CEA/DAM au terme de l'exécution du Marché.

11 Audits du CEA

Le CEA/DAM et son autorité de sécurité se réservent le droit de procéder ou de faire procéder à un ou plusieurs audits pour vérifier la bonne application des présentes dispositions.

Chapitre 3 : Prescriptions pour les échanges d'informations sensibles non classifiées

1 Objet

Le présent chapitre précise les exigences du CEA liées à la sécurité des échanges d'information ou de supports dans les projets/marchés du CEA/DAM réalisés avec des partenaires industriels. Le présent document vient en application des obligations déclinées dans le Plan Contractuel de Sécurité (PCS) du Marché, qui définit le niveau de classification ou, le cas échéant de protection du Marché et la sensibilité de ses composantes informationnelles.

2 Terminologie

Le glossaire est joint en annexe des présentes dispositions.

3 Echanges avec le CEA/DAM

3.1 – Messagerie électronique

Dans le cadre de l'exécution du Marché, les personnels du Titulaire et de ses sous-traitants/cotraitants éventuels sont amenés à communiquer par messagerie électronique entre eux, et avec les acteurs CEA/DAM, des pièces jointes de niveau DR (sensible non classifié de défense). Ces pièces jointes doivent être transmises dans des conteneurs chiffrés avec le logiciel de chiffrement ACID Cryptofiler ou avec le logiciel de chiffrement ZoneCentral (conteneurs Zed).

Aucun message de niveau DR (corps du message et pièce jointe) n'est transmis en clair sur Internet.

La communication par messagerie électronique de pièces jointes de niveau classifié de défense est strictement interdite.

3.2 – Réunions

Dans le cadre des réunions liées au Marché, la connexion d'un support amovible ou d'un ordinateur portable non CEA/DAM sur un réseau CEA/DAM est strictement interdite ou soumise à autorisation préalable du CEA/DAM.

Pour les présentations en salles de réunion du CEA, les présentations doivent être préalablement transmises au CEA. A titre de dérogation et sous réserve de l'accord préalable du CEA/DAM le Titulaire peut venir avec son ordinateur portable professionnel¹³ qui peut être connecté directement sur un vidéoprojecteur.

Les téléphones portables sont interdits sur la plupart des Centres du CEA/DAM¹⁴, il convient de se conformer sur ce sujet en particulier au règlement intérieur de chaque Centre, en vigueur à la date de la réunion. Si la réunion a lieu en dehors du CEA/DAM et traite d'informations sensibles ou classifiées, le responsable CEA de la réunion peut interdire la présence de téléphone portable dans la salle ainsi que la prise de note sur support informatique ou papier.

3.3 – Intervention sur Centre CEA/DAM

Dans le cadre des interventions liées au Marché, la connexion d'un support amovible ou d'un ordinateur portable non CEA/DAM sur un réseau CEA/DAM est interdite sauf nécessité impérieuse approuvée préalablement par le CEA/DAM.

¹³ Pour rentrer du matériel (ordinateur ou support amovible) sur un centre CEA/DAM, une demande doit préalablement être faite auprès du responsable CEA du marché et validée par l'Officier de Sécurité (OS) du centre.

¹⁴ Les téléphones doivent être déposés dans des casiers consigne à l'entrée des centres.

Dispositions applicables aux Titulaires de marchés passés par le CEA/DAM en matière de protection de l'information *Diffusion Restreinte*

Pour les opérations sur site en phase d'intégration des systèmes informatiques et industriels de l'affaire, le Titulaire doit prévoir les moyens matériels et logiciels qui devront rester sur site pendant la durée des travaux. Il est admis qu'un support amovible dédié à cette activité, jamais connecté à Internet et vérifié sain en usine, soit utilisé comme navette entre le réseau spécifique et l'installation sur site.

En prévision des activités de MCO (Maintien en Condition Opérationnelle), le Titulaire doit définir la configuration informatique nécessaire pour disposer des moyens in-situ afin d'assurer la maintenance des systèmes informatiques et industriels livrés, sans devoir faire rentrer du matériel informatique non maîtrisé par le CEA/DAM.

4 Logiciels de chiffrement de conteneur

Le CEA/DAM choisit le logiciel de chiffrement de conteneurs utilisé pour les échanges sensibles non classifiés entre le Titulaire et le CEA/DAM. Le choix de technologie est entre :

- Par principe Zed : ce sont des conteneurs chiffrés produits par les logiciels ZoneCentral et Zed dans leurs versions qualifiées par l'ANSSI. Si le Titulaire ne possède pas ces logiciels, le logiciel Zedle est mis à disposition gratuitement au Titulaire via un site Internet d'accès libre (cf §3 du chapitre 1 et guide en annexe 2). Le CEA/DAM choisit d'utiliser des clés délivrées gratuitement par l'infrastructure de gestion de clés du CEA/DAM ou un code d'accès par mot de passe défini en concertation avec le Titulaire et respectant les règles de constitution du CEA/DAM.
- A titre exceptionnel ACID, si le Titulaire dispose déjà du logiciel : ce sont des conteneurs chiffrés produits par le logiciel ACID Cryptofiler qui est un produit qualifié par l'ANSSI et de distribution contrôlée. Les clés sont fournies par un organisme agréé pour la distribution de clés ACID du domaine cryptographique 'INDUS'.
-

5 Audits du CEA

Le CEA/DAM et son autorité de sécurité se réservent le droit de procéder ou de faire procéder à un ou plusieurs audits pour vérifier la bonne application des spécifications des présentes dispositions.

Annexe 1 - Glossaire

ACID	Logiciel de chiffrement de conteneurs
ANSSI	Agence nationale de la sécurité des systèmes d'information
CD	Confidentiel-Défense (mention), ancienne terminologie de l'IGI 1300, remplacée par Secret
Centre	Tout site du CEA/DAM
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CEA/DAM	Direction des applications militaires du CEA
DSSN	Direction de la sécurité et de la sûreté nucléaire du CEA
DO	Diffusion ordinaire
DR	<i>Diffusion Restreinte</i> (mention)
GSM	Global System for Mobile communications (connexion téléphonie mobile)
ISC	Information ou support classifié
ISP	Information ou support protégé
OSSI-C	Officier de sécurité des systèmes d'information du Centre
PDA	Personal Digital Assistant (Assistant personnel ou Ordinateur de poche)
RSSI	Responsable de la sécurité des systèmes d'information
S	Secret (classification), nouvelle terminologie de l'IGI 1300
SD	Secret Défense, ancienne terminologie de l'IGI 1300, remplacée par Très Secret
SI	Système(s) d'information
SSI	Sécurité des systèmes d'information
TS	Très Secret (classification), nouvelle terminologie de l'IGI 1300
USB	Universal Serial Bus
Wi-Fi	Accès réseau sans fil (différents protocoles utilisés : WPA soit Wi-Fi Protected Access, WPA2 (préconisé), WPA3)
Zed	Conteneurs chiffrés
Zedle	Logiciel d'utilisation de conteneurs chiffrés, associé à ZoneCentral
ZoneCentral	Logiciel de chiffrement de poste de travail

Annexe 2 - Guide d'utilisation de la version Zed Limited Edition à date

Une fois que vous avez cliqué sur le lien <https://client.primx.eu/PublicSoftware/zedlimitededition/>, sélectionnez la version correspondante à votre système d'exploitation et à la version souhaitée :

ZED!
LIMITED EDITION

Vous avez reçu un conteneur chiffré avec l'extension zed ?

ZED! LIMITED EDITION est la solution pour ouvrir des conteneurs chiffrés et compressés

Pour partager des documents de manière sécurisé sous forme de conteneur, vos partenaires utilisent ZED!, la solution de chiffrement de fichiers de PRIM'X.

Avec ZED! LIMITED EDITION vous pouvez :

- + Ouvrir des conteneurs .zed chiffrés par vos partenaires ou vos clients.

ZED! LIMITED EDITION est disponible gratuitement en téléchargement

Système: Windows

Version: Version 2022.4 - Windows 64 bits

Télécharger

Signature : 04 20 4B 19 19 F1 67 3F 03 39 53 8E EB 8A B5 53 12 00 1C 03 82 6D 34 6C E8 E4 F2 2C 38 77 D5 48 FE 93

Une fois le téléchargement terminé ouvrez le fichier et lancez le fichier téléchargé, soit dans l'exemple ci-dessus **Z!** zedle Q.2020.1 x64.exe

Dans le logiciel ouvert sélectionnez votre fichier xxx _DR.zed puis insérez le mot de passe.