

Clause de Sécurité des Systèmes d'Information (SSI)

Réf : RI.84 - Clausier de sécurité des marchés publics pour la DGAP

Table des matières

Synthèse du document	2
Préambule	2
Objectifs	2
Article 1 : Sécurité des Systèmes d'Information (SSI).....	3
1.1. Cadre de référence et conformité réglementaire.....	3
Article 2 : Plan d'Assurance Sécurité (PAS).....	3
Article 3 : Confidentialité et Accord de Non-Divulcation (AND)	4
Article 4 : Contrôle d'accès et habilitations du personnel	4
Article 5 : Droit d'audit, inspections et contrôles.....	4
Article 6 : Gestion des incidents de sécurité et des compromissions	5
Article 7 : Réversibilité, restitution et destruction sécurisée des données.....	5

Synthèse du document

Ce document constitue les clauses de Sécurité des Systèmes d'Information (SSI). Elles formalisent les exigences de sécurité applicables aux titulaires et à leurs sous-traitants de tous rangs. Ses dispositions couvrent la conformité réglementaire (PSSI Sûreté, RGPD, IGI 1300, II 901), la gouvernance de la sécurité via le Plan d'Assurance Sécurité (PAS), les accords de confidentialité (AND), la gestion rigoureuse des accès physiques et logiques, la vérification par audit, les protocoles de réaction aux incidents (notamment l'isolation logique sans extinction de l'équipement compromis) ainsi que les procédures de réversibilité et de destruction ou blanchissement sécurisé des données en fin de contrat.

Préambule

Objectifs

La Direction Générale de l'Administration Pénitentiaire (DGAP) met en œuvre des systèmes d'information de sûreté et de traitement de données hautement critiques, dont la compromission pourrait impacter directement la sécurité des établissements, des personnels et du public.

L'intégration de ces clauses de sécurité poursuit des objectifs fondamentaux et indissociables :

1. **Garantir la souveraineté et la protection des secrets** : Assurer un niveau de sécurité conforme aux obligations nationales (protection des informations classifiées ou de niveau *Diffusion Restreinte*) en encadrant les échanges et la manipulation des données par des tiers.
2. **Sanctuariser les infrastructures physiques et logiques** : Imposer un cloisonnement étanche des réseaux et des locaux techniques pour prémunir l'administration contre toute tentative d'intrusion, de sabotage ou d'interception.
3. **Assurer la résilience et la continuité de service public** : Exiger du titulaire une haute disponibilité et des plans de secours testés pour minimiser l'impact de toute défaillance ou sinistre cyber sur l'activité opérationnelle des sites.
4. **Tracer, auditer et responsabiliser** : Établir une imputabilité totale et une traçabilité probante de chaque action technique pour permettre le contrôle permanent de l'état de sécurité et la conduite d'investigations en cas d'anomalie.
5. **Maîtriser le cycle de vie de la donnée** : Garantir que l'administration conserve la pleine maîtrise et propriété de ses données, de la conception à la réversibilité, en excluant tout risque de rétention ou de fuite d'informations sensibles à la fin des prestations.

Article 1 : Sécurité des Systèmes d'Information (SSI)

1.1. Cadre de référence et conformité réglementaire

Le titulaire conçoit, met en œuvre, héberge et exploite les systèmes d'information fournis pour le compte de l'Administration et sous sa responsabilité conformément au cadre réglementaire et aux politiques de sécurité en vigueur.

Le titulaire s'engage contractuellement à respecter, et à faire respecter par ses éventuels sous-traitants, les référentiels de sécurité applicables suivants :

1. **La Politique de Sécurité des Systèmes d'Information (PSSI) Sûreté de la DGAP (RI.01)**, ses volets transverse, infrastructure et spécifiques, ainsi que ses évolutions tout au long de l'exécution du contrat.
2. **Le Règlement Général sur la Protection des Données (RGPD)** et la **Loi Informatique et Libertés (LIL)** pour tout traitement de Données à Caractère Personnel (DCP).
3. **L'instruction générale interministérielle n° 1300 (IGI 1300)** sur la protection du secret de la défense nationale.
4. **L'instruction interministérielle n° 901 (II 901)** relative à la protection des systèmes d'information traitant d'informations sensibles non classifiées de niveau *Diffusion Restreinte* (DR).
5. **Le Référentiel Général de Sécurité (RGS)** et le **Référentiel Général d'Interopérabilité (RGI)** en vigueur.

Le titulaire dispose d'un délai maximal de **trois (3) mois** après la transmission d'une mise à jour de la PSSI de la DGAP pour présenter ses déclarations de conformité et de **six (6) mois** pour l'intégrer pleinement dans le pilotage des prestations.

Article 2 : Plan d'Assurance Sécurité (PAS)

Le titulaire a l'obligation de formaliser et de maintenir à jour un **Plan d'Assurance Sécurité (PAS)**, conforme au modèle de la DGAP [RM.15].

- **Dépôt initial** : Le projet de PAS doit être soumis à l'approbation de la DGAP au moins **trente (30) jours** avant le démarrage effectif des prestations.
- **Approbation** : Les prestations ne pourront débuter qu'après l'approbation formelle et écrite du PAS par le Responsable Central de la Sécurité des Systèmes d'Information (RCSSI) de la DGAP.
- **Évolutions et Revue** : En cas de changement majeur du système d'information, de son architecture ou de l'environnement de la prestation, une revue du PAS sera menée conjointement.

Le représentant légal du titulaire est personnellement responsable du respect des engagements de sécurité décrits dans le PAS approuvé durant toute la durée du marché.

Article 3 : Confidentialité et Accord de Non-Divulgence (AND)

L'ensemble des documents, données, plans de réseaux, plans bâtimentaires et configurations techniques liés au système d'information de l'Administration sont classés au minimum au niveau **DIFFUSION RESTREINTE**.

- **Accord de Non-Divulgence Global (AND) :** Le titulaire doit signer un Accord de Non-Divulgence global conforme au modèle **[RM.22]** de la DGAP dès la notification du marché.
- **Engagements Individuels :** Le représentant du titulaire s'engage à faire signer un accord de non-divulgence individuel ou une charte d'utilisation des SI de la DGAP (reprenant *a minima* les engagements de confidentialité avec la DGAP) à chaque collaborateur (interne ou sous-traitant) affecté au marché avant toute affectation de droits ou d'accès.

Article 4 : Contrôle d'accès et habilitations du personnel

L'accès aux ressources logiques et physiques de l'Administration est strictement régi par le principe du moindre privilège.

- **Contrôle élémentaire et Habilitations :** Tout intervenant du titulaire nécessitant des droits d'administration ou l'accès à des données sensibles doit faire l'objet d'une procédure de contrôle élémentaire (casier judiciaire B2 pour les ressortissants français, vérifications équivalentes pour les ressortissants étrangers). Si la mission implique l'accès à des informations classifiées, l'obtention préalable de l'habilitation « **SECRET** » correspondante est un prérequis impératif à toute prise de fonction.
- **Dossier Administratif [RM.05] :** Un dossier administratif individuel conforme au modèle **[RM.05]** doit être instancié pour chaque intervenant du titulaire, identifiant de manière exhaustive ses droits d'accès réseau, ses badges et le matériel informatique attribué.
- **Registre du personnel [RM.16] :** Le titulaire s'engage à fournir et maintenir à jour la liste nominative de ses collaborateurs devant intervenir sur le système d'information de sûreté. Cette liste est consignée dans le registre **[RM.16]** et fait l'objet d'une revue périodique contradictoire.

Article 5 : Droit d'audit, inspections et contrôles

Le titulaire s'engage à accepter, sur simple demande, des audits de sécurité menés par la DGAP ou par tout organisme tiers qualifié mandaté par elle (prestataires qualifiés PASSI de l'ANSSI notamment).

- **Disponibilité des ressources :** Le titulaire garantit la mise à disposition des ressources humaines, techniques et documentaires nécessaires à la conduite de l'audit dans un délai maximal de **trois (3) mois** suivant la notification de la demande d'audit par la DGAP.

- **Traitement des écarts** : En cas d'écarts constatés par rapport aux exigences du marché ou du PAS, le titulaire présentera un plan de remédiation sous **quinze (15) jours**. Les coûts de remédiation des non-conformités imputables au Titulaire restent à sa charge exclusive.

Article 6 : Gestion des incidents de sécurité et des compromissions

Le titulaire s'engage à notifier sans délai à la chaîne SSI de la DGAP (RISSI / RCSSI) tout incident de sécurité ou toute suspicion de compromission physique ou logique survenue sur son périmètre ou susceptible d'affecter le SI de l'Administration.

En cas de compromission confirmée, le Titulaire s'engage à :

1. **Isoler immédiatement** l'élément compromis logiquement en le déconnectant de tout réseau, **sans l'éteindre** afin de préserver les données volatiles en mémoire vive (RAM) nécessaires à l'investigation numérique conformément aux consignes **[RI.23]** et **[RI.64]**.
2. **Isoler physiquement** les équipements ou supports concernés (mise sous scellés).
3. **Collaborer activement** avec les équipes d'investigation désignées par l'Administration (prestataires qualifiés PRIS de l'ANSSI notamment) et fournir l'ensemble des journaux d'événements et traces techniques.
4. Consigner chronologiquement l'ensemble des actions et communications dans une main courante de gestion de crise sur la base du modèle **[RM.32]**.

Article 7 : Réversibilité, restitution et destruction sécurisée des données

Conformément à l'exigence de réversibilité, à l'expiration ou en cas de résiliation du contrat, le Titulaire garantit qu'aucune donnée de l'Administration ne pourra être conservée sur son propre système d'information.

- **Restitution des matériels** : Tout équipement ou support de stockage mis à disposition par la DGAP devra être physiquement restitué et fera l'objet d'un procès-verbal de remise et restitution des actifs conforme au modèle **[RM.01]**. Ce PV est conservé durant **cinq (5) ans** par l'Administration.
- **Blanchissement et Destruction** : L'effacement sécurisé de l'ensemble des données de l'Administration sur les supports appartenant au titulaire doit être réalisé selon un procédé conforme à la procédure **[RI.10]** (normes techniques ANSSI de destruction et de blanchissement). En cas d'impossibilité technique ou de panne de l'équipement empêchant un effacement logique, le support physique (disque dur, mémoire flash) devra faire l'objet d'une **destruction physique sur site** (broyage ou démagnétisation) sous le contrôle d'un agent de la DGAP avant sa mise au rebut ou son emport par un tiers. Un PV de destruction sera rédigé et co-signé par les Parties.