

**Plan d’Assurance Sécurité**

**[NOM\_DU\_PRESTATAIRE]**

**[Référence du marché ou de l’accord-cadre]**

**Version X.Y**

Historique des modifications

| Version | Date | Auteur(s) – Entité | Description |
| --- | --- | --- | --- |
| 0.1 | JJ/MM/AAAA |  | Création du document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Validation du document

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom Prénom** | **Entité** | **Fonction** | **Date** |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |

Diffusion du document

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom Prénom** | **Entité** | **Fonction** | **Date** |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |
|  |  |  | JJ/MM/AAAA |

Table des matières

[1. Principes généraux 6](#_Toc78995241)

[2. Responsabilités 7](#_Toc78995242)

[2.1. Etablissement du PAS 7](#_Toc78995243)

[2.2. Mise en application et suivi du PAS 7](#_Toc78995244)

[2.3. Diffusion du PAS 7](#_Toc78995245)

[2.4. Revue annuelle du PAS 7](#_Toc78995246)

[2.5. Evolution du PAS 7](#_Toc78995247)

[2.6. Organisation de la sécurité du PAS 7](#_Toc78995248)

[3. Applicabilité du PAS 10](#_Toc78995249)

[3.1. Condition d’application 10](#_Toc78995250)

[3.2. Non-respect du PAS 10](#_Toc78995251)

[3.3. Demande de dérogation 10](#_Toc78995252)

[4. Documents Applicables et de Référence 11](#_Toc78995253)

[4.1. Documents applicables 11](#_Toc78995254)

[4.2. Documents de référence 11](#_Toc78995255)

[5. Description de la Prestation 12](#_Toc78995256)

[5.1. Généralités 12](#_Toc78995257)

[5.2. Lieux d’exécution 12](#_Toc78995258)

[6. Synthèse des exigences du Client 13](#_Toc78995259)

[7. Indicateurs de sécurité 14](#_Toc78995260)

[8. Mesures de sécurité 15](#_Toc78995261)

[8.1. Politique de sécurité de l’information 15](#_Toc78995262)

[8.2. Organisation de la sécurité de l’information 15](#_Toc78995263)

[8.3. Sécurité des ressources humaines 17](#_Toc78995264)

[8.4. Sécurité des actifs 18](#_Toc78995265)

[8.5. Contrôle d’accès 19](#_Toc78995266)

[8.6. Cryptographie 21](#_Toc78995267)

[8.7. Sécurité physique et environnementale 21](#_Toc78995268)

[8.8. Sécurité liée à l’exploitation 22](#_Toc78995269)

[8.9. Sécurité des communications 24](#_Toc78995270)

[8.10. Acquisition, développement et maintenance des systèmes d’information 25](#_Toc78995271)

[8.11. Relations avec les fournisseurs 26](#_Toc78995272)

[8.12. Gestion des incidents liés à la sécurité de l’information 27](#_Toc78995273)

[8.13. Organisation et mise œuvre de la continuité de la sécurité de l’information 28](#_Toc78995274)

[8.14. Conformité 29](#_Toc78995275)

[8.15. Homologation 30](#_Toc78995276)

[8.16. Analyse de risque stratégique 31](#_Toc78995277)

[9. Matrice de couverture des exigences de sécurité 32](#_Toc78995278)

[10. Annexe 33](#_Toc78995279)

[10.1. Glossaire 33](#_Toc78995280)

[10.2. Conformité PSSI-MI 34](#_Toc78995281)

**Préambule**

Ce document constitue un modèle de plan d’assurance sécurité.

A ce titre, il peut être utilisé par les directions et services du ministère dans le cadre d’un marché ou d’un accord cadre pour :

* Imposer un plan d’assurance sécurité aux soumissionnaires dès le lancement du marché et ainsi ne retenir que ceux aptes à répondre à ces exigences ;
* Proposer un modèle type à fournir aux soumissionnaires d’un appel d’offre ou aux titulaires d’un marché, permettant de s’assurer de l’exhaustivité des mesures proposées vis-à-vis des attentes du ministère en matière de sécurité numérique. Le soumissionnaire ou le titulaire pourra s’en inspirer pour compléter des rubriques potentiellement manquantes dans son propre plan d’assurance sécurité.

Le document s’adresse à tous les types de prestations : développement, hébergement AMOA, etc.

**Chaque prestataire devra retenir et compléter les seules mesures adaptées à la prestation dans le chapitre 9 « Mesures de sécurité ». La mention "Sans Objet" devra être indiquée à toutes les mesures non applicables de la prestation.**

# Principes généraux

Un PAS a pour but de préciser comment la société [Nom de la société du prestataire] (ci-après désigné le « Prestataire ») se conforme aux exigences de cybersécurité définies par [Nom de l’entité du MI] (ci-après désigné le « Client »). Chaque cotraitant ou sous-traitant auquel le Prestataire peut avoir recours doit être conforme avec aux règles édictées dans son propre PAS.

En pratique, il est l’équivalent du Plan d’Assurance Qualité (PAQ) sur le volet sécurité de la prestation. A ce titre, il répond aux besoins de sécurité des produits ou services à fournir au titre de la prestation, exprimés par le Client.

Ce document décrit les dispositions que le Prestataire s’engage à mettre en œuvre pour répondre :

* Aux risques que le Prestataire a identifiés sur ses services mutualisés/transverses utilisés dans le cadre de toutes ou parties de ses prestations ;
* Aux exigences de sécurité du Client dans le cadre des éléments contractuels de la prestation ;
* Aux éventuels risques que le Client a identifié sur ses systèmes d’information faisant l’objet de la prestation.

Il définit en particulier l’organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité de la prestation et les mesures techniques, organisationnelles et procédurales mises en œuvre. Il constitue :

* Un outil de travail et un référentiel commun à tous les acteurs pour leur donner une vision similaire du Projet ;
* Le cahier des charges de la sécurité, réalisé en collaboration avec le Client et approuvé par lui ; chaque partie se doit donc de le respecter.

Le PAS doit être un document précis, concis et réaliste. Les prescriptions qu'il contient devront être suffisamment simples pour être applicables facilement et pour que leur application soit aisément vérifiée.

Ce document est destiné :

* Au Client à qui le PAS présente les dispositions mises en œuvre par le Prestataire mais aussi les actions et produits attendus de sa part ;
* Aux auditeurs (internes ou externes) afin qu’il serve de référence, lors de l’évaluation de la conformité entre ce qui est écrit et ce qui est réellement mis en œuvre sur le Projet.

# Responsabilités

## Etablissement du PAS

Le PAS est défini conjointement entre le Client et le Prestataire. Il est le référentiel commun en matière de sécurité numérique tout au long de la relation contractuelle.

Le Prestataire organise les réunions de travail nécessaires avec le Client pour finaliser et rédiger le PAS. Le Client valide la version finale qui sera annexée au contrat. La première version approuvée et applicable du PAS porte le numéro 1.0.

## Mise en application et suivi du PAS

Le Prestataire est responsable de la mise en application du PAS par chacun des intervenants. Afin d’assurer la protection des éléments sensibles liés à la prestation, le Prestataire vérifie sa mise en œuvre et contrôle de manière directe l’application des exigences de sécurité du Client.

Le RSSI du Client est responsable de l’application du PAS pour les actions relevant de son domaine. Il en contrôle l'application, relève les anomalies de fonctionnement, arbitre en cas de conflit entre le Client et le Prestataire sur un des éléments du PAS.

## Diffusion du PAS

Les responsables de projet du Prestataire et du Client sont responsables de la diffusion du PAS dans leurs entités, et notamment à l'ensemble des personnes citées en page de garde.

## Revue annuelle du PAS

Le Prestataire doit effectuer au moins une revue annuelle du PAS afin de s’assurer de l’absence d’écart entre les pratiques décrites dans le document et celle qu’il réalise. À l’issue de la revue, un compte rendu circonstancié est transmis à l’acheteur.

Dans le cas où des écarts sont identifiés, le Prestataire propose les corrections à apporter et les soumet à l’acheteur pour validation.

## Evolution du PAS

Lorsqu’une révision du PAS est rendue nécessaire par l’évolution du cadre légal ou réglementaire, ou par une modification de la prestation (périmètre, exigence du Client…), le Prestataire fait évoluer les éléments décrits dans ce PAS.

Chaque évolution fait l'objet d'une évolution du numéro de version et soumise au comité de pilotage de la prestation qui statue sur son acceptation ou son refus, acté dans un compte-rendu de réunion. Toute évolution du PAS fait partie de celui-ci et engage les parties au même titre.

## Organisation de la sécurité du PAS

### Responsabilité

Le PAS est rédigé et mis à jour par le Prestataire, et validé par le Client.

Le Responsable Projet du Prestataire :

* Est responsable, avec l’aide de son RSSI et celui du Client, de la sélection des dispositions prévues dans le PAS du projet, il veille particulièrement à la pertinence du PAS par rapport aux exigences du contrat et le fait approuver en interne, puis formellement par le Client.
* Veille à ce que toutes les dispositions prévues au PAS soient appliquées et efficaces. L’atteinte des objectifs est vérifiée au travers de contrôles sécurité et indicateurs ;
* Est responsable de l’évolution des dispositions et donc du présent PAS en fonction des changements du projet et du contexte d’exécution de la prestation.

### Organisation du Prestataire

|  |
| --- |
| Responsable Projet : |
| [Décrire les rôles et actions] |
| RSSI |
| [Décrire les rôles et actions] |

### Organisation du Client

|  |
| --- |
| Responsable(s) de la prestation |
| [Décrire les rôles et actions, par exemple   * S’assure, en lien avec son RSSI, que toutes les dispositions en matière de sécurité ont été prises par le Prestataire pour mener à bien la prestation * Demande l’évolution du PAS en fonction des changements liés à la prestation * Pilote et organise les comités de pilotage   Pour des marchés à multiples SI, le responsable de la prestation peut déléguer localement ses missions à des chefs de projet. |
| RSSI |
| [Décrire les rôles et actions, par exemple :   * S’assure du respect des démarches sécurité dans le cadre de la prestation * Conseille le responsable de la prestation sur les aspects de sécurité * Valide les documents de sécurité * Contrôle l’application du PAS et propose les audits à conduire (si pertinent par rapport à la prestation) * Participe au comité de pilotage] |

### Instance de pilotage

Le pilotage de la sécurité se fait dans les instances de pilotage définies pour la prestation.

Les points suivants y sont traités :

* La validation des documents relatifs à la sécurité ;
* La mise en œuvre des dispositions de sécurité applicables ;
* Le suivi des tableaux de bord sécurité élaborés par le Prestataire ;
* Le suivi des plans d’action ;
* Le règlement des litiges éventuels concernant la sécurité ;
* Le lancement des opérations de contrôle et d’audits de sécurité (si pertinent);
* L’analyse des résultats des audits de sécurité et les propositions de mesures correctives (si pertinent) ;
* Le suivi de la gestion des risques.

# Applicabilité du PAS

## Condition d’application

Le PAS s’applique à toutes les activités mentionnées dans le contrat et à l’ensemble des équipes du Prestataire chargées de la prestation, au même titre que le Plan d’Assurance Qualité et avec la même priorité.

[Si prestation de développement et/ou d’hébergement, préciser les environnements faisant partis de la prestation : production, pré-production, qualification, test]

## Non-respect du PAS

L’application effective du PAS et son efficacité font l’objet de vérifications et d’un suivi régulier exercé par le Prestataire et le Client.

Un acteur du projet identifiant un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement au RSSI du Prestataire, qui escaladera au Client.

En cas de non-respect constaté, le Prestataire et le Client décident :

* Soit de proposer une évolution du PAS, en cas de constat de procédure non adaptée, via une demande de dérogation ;
* Soit de demander l'application stricte du PAS.

## Demande de dérogation

Toute demande de dérogation vis à vis des exigences du PAS devra être instruite par le Prestataire et le Client, et soumise à l’approbation du comité de pilotage de la prestation, qui statut sur :

* Une dérogation définitive qui implique à terme une évolution du PAS ;
* Une dérogation temporaire, avec précision de la durée.

La décision est actée dans le compte-rendu du comité.

# Documents Applicables et de Référence

## Documents applicables

Liste des documents strictement applicables (documents contractuels, livrables, procédures, etc.).

|  |  |  |
| --- | --- | --- |
| **Sources**  **(Client / Prestataire)** | **Référence du document** | **Intitulé du document** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Documents de référence

Liste des documents de sécurité qui garantissent par contrôle, l’alignement du Prestataire aux normes et à la réglementation en matière de sécurité des systèmes d’information pour la mise en œuvre des mesures de sécurité de la prestation.

|  |  |  |
| --- | --- | --- |
| **Sources**  **(Client / Prestataire)** | **Référence du document** | **Intitulé du document** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Description de la Prestation

## Généralités

<A Compléter>

## Lieux d’exécution

<Indiquer le ou les lieux où sont effectuées les prestations. S’il s’agit de prestations de développement ou d’hébergement notamment, préciser aussi le pays>

<Décrire de manière plus précise la prestation : les architectures techniques et fonctionnelles (si concernées), les livrables attendus, les réunions ou ateliers prévus etc.>

# Synthèse des exigences du Client

<Indiquer la ou les références vers un ou des documents du Client indiquant toutes les exigences de sécurité demandées.

Préciser les exigences supplémentaires demandées qui ne seraient pas dans les documents (exprimées lors de la réunion de cadrage, etc.).>

# Indicateurs de sécurité

<Indiquer tous les indicateurs qui seront fournis par le Prestataire au client. Le Client peut demander à ce que soient rajouter d’autres indicateurs s’il le juge nécessaire.

Indiquer le format de livraison (portail dédié du Prestataire, courriel pour des documents PDF, Excel, etc.). Préciser les destinataires de ces indicateurs et la périodicité de mise à jour ou d’envoi>

# Mesures de sécurité

Les mesures ci-dessous sont mises en place par le Prestataire pour assurer la protection de la prestation et notamment en réponse aux exigences du Client.

Ce PAS détaille les mesures de sécurité spécifiques qui s’appliquent dans le contexte du projet pour le compte du Client.

## Politique de sécurité de l’information

Le Prestataire a défini une Politique de Sécurité des Systèmes d’Information qui décrit les principes généraux de sa politique de sécurité des systèmes d’information.

<Indiquer la référence de la PSSI du Prestataire. Cette PSSI sera jointe au PAS lorsque ce dernier sera envoyé au Client.

Indiquer la périodicité de la révision de la PSSI du Prestataire>

## Organisation de la sécurité de l’information

### Organisation interne

* + - 1. Fonctions et responsabilités liées à la sécurité de l’information.

<Ce paragraphe décrit les rôles, les responsabilités et l’organisation de la chaîne fonctionnelle Sécurité SI du Prestataire.>

* + - 1. Séparation des tâches

Les tâches et les domaines de responsabilité incompatibles sont cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs du prestataire et de la maîtrise d’ouvrage.

L’organisation de la SSI repose sur le principe de la séparation des pouvoirs. Les fonctions de décision et de contrôle permanent sont placées sous la responsabilité du [Rôle(s) / Fonction(s)].

Il existe également une séparation des rôles dans le projet. Ainsi :

* Les différents rôles dans le projet sont assurés par des personnes différentes : une séparation effective des tâches opérationnelles (individus et responsabilités) existe entre développement, intégration applicative, administration système, administration réseaux, administration des bases de données, ingénierie système, ingénierie réseau, exploitation ;
* Les trois catégories d’opérations suivantes sont indépendantes :
  + conception et développement,
  + tests et qualification,
  + mise en production et exploitation ;
* Les développeurs et les équipes métier/études n’ont pas accès aux environnements de production ;
* Les actions d’administration réseau sont coordonnées avec les opérations d’administration des systèmes afin de garantir la consistance des protections et la continuité des opérations ;
  + Les administrateurs réseaux et systèmes appartiennent à deux équipes distinctes et le cumul de ces rôles n’est pas autorisé ;
* L’accès aux outils et utilitaires sensibles, qui servent à l’exploitation du service, est limité et contrôlé ;
* L’acquisition et l’utilisation de nouveaux outils et utilitaires réseau sont soumises à l’accord du responsable compétent ;
* La documentation système est accessible aux seules personnes ayant besoin de la connaître ;
* Les environnements de développement, de test et de recette sont totalement séparés des environnements de production.

### Relation avec les autorités

<Décrire :

* Les organismes dont lesquels le Prestataire est membre ;
* Les ministères ou acteurs institutionnels avec lesquels il travaille>

### Relations avec des groupes de travail spécialisés

<Décrire :

* Les groupes d’intérêt, les forums, les associations professionnelles spécialisés dans la sécurité dont lesquels le Prestataire est membre.
* Les abonnements à des organismes de veille en lien avec la sécurité numérique que le Prestataire possède>

### La sécurité de l’information dans la gestion de projet

<Décrire ou indiquer si une politique de sécurité du Prestataire traite l’attendu en matière de sécurité via par exemple :

* Les principes généraux : protection des informations du projet, gestion documentaire, séparation des environnements, séparation de rôles dans le projet ;
* Des règles de cadrage concernant l’évaluation des enjeux de sécurité et des impacts sur la vie privée ;
* Les règles de conceptions : évaluation de la conformité réglementaire, évaluation des besoins de sécurité, intégration de la sécurité dans les spécifications fonctionnelles, intégration de la sécurité dans les spécifications techniques ;
* Les règles de réalisation : respect des spécifications, accès aux environnements de développement, sensibilisation aux risques de sécurité des applicatifs, contrôles de sécurité dans les applicatifs, intégration de code tierce partie, protection des codes sources, droits de propriété intellectuelle ;
* Les règles de test : données de tests, tests de sécurité ;
* Les règles de déploiement et d’évolution : déploiement en production, intégration de la sécurité dans les modifications / évolutions ;
* Les règles pour des achats de solutions externes à intégrer aux projets.

Le Prestataire précise s’il a mis en place un Système de management de la Sécurité de l’Information (SMSI) selon l’ISO 27001 et indique le cas échéant sa déclaration d’applicabilité.>

### Appareils mobiles et télétravail

* + - 1. Appareils mobiles

<Décrire les mesures spécifiques adoptées pour gérer les risques découlant de l’utilisation des appareils mobiles, telles que :

* Les stations de travail : durcissement, accès nominatifs et sans privilège, ports USB désactivés ou enrôlement des périphériques ;
* Le réseau virtualisé : accessibilité uniquement depuis les réseaux publics que via un VPN du Prestataire ;
* L’accessibilité au VPN : une authentification double facteur, un processus d’habilitation.
* L’autorisation ou non d’utiliser des terminaux personnels pour accéder à la messagerie ;
* etc. >
  + - 1. Travail à distance

<Décrire la politique en matière de télétravail du Prestataire>

## Sécurité des ressources humaines

### Avant l’embauche

* + - 1. Sélection des candidats

<Décrire les processus du Prestataire, notamment quels points sont demandés et vérifiés selon les candidats, dans le respect de la règlementation en vigueur.>

* + - 1. Termes et conditions d’embauche

<Décrire les processus du Prestataire, notamment les clauses de confidentialités et/ou d’habilitation.>

### Pendant la durée du contrat

* + - 1. Responsabilité de la direction

La direction de projet du Prestataire s’engage à communiquer le présent PAS à l’ensemble des intervenants du projet, salariés comme sous-traitants conformément aux politiques et aux procédures en vigueur, et de s’assurer du respect de l’ensemble des exigences sécurité qui y sont précisées.

<Indiquer les mesures prises par la direction. Préciser le processus d’information envers les sous-traitants>

* + - 1. Sensibilisation, apprentissage et formation à la sécurité de l’information

L’ensemble des salariés du Prestataire et, quand cela est pertinent, des sous-traitants, bénéficient d’une sensibilisation et de formations adaptées et ainsi que de leurs mises à jours.

En outre, l’ensemble des salariés du Prestataire et tous les sous-traitants intervenant sur le projet sont sensibilisés et formés par l’intermédiaire :

* <Lister les différentes actions de sensibilisation et formation>

<Lister les actions et mesures complémentaires de formation et sensibilisation>

* + - 1. Processus disciplinaire

<Décrire le processus disciplinaire>

Le non-respect des règles décrites dans la <charte utilisateur> engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables et l'expose éventuellement, de manière appropriée et proportionnée au manquement commis, aux sanctions disciplinaires définies par le Règlement Intérieur.

<Rappel des sanctions du règlement intérieur>

* + - 1. Revue des compétences

Le Client peut sur simple demande consulter les compétences des personnels du Prestataire intervenant sur son périmètre.

Il appartient au Prestataire de fournir au Client tous les éléments permettant cette vérification (CV, preuve de formation, etc.).

### Rupture, terme ou modification du contrat de travail

* + - 1. Achèvement ou modification des responsabilités associées au contrat de travail

<Décrire le processus associé : modification / restitutions des actifs, modification / suppression des droits d’accès, etc.>

## Sécurité des actifs

### Responsabilité relative aux actifs

* + - 1. Inventaire des actifs

<Décrire le processus d’inventaire des actifs. Définition des propriétaires de chaque actifs et règles associées.>

* + - 1. Classification des informations

<Décrire le processus de classification des informations>

* + - 1. Marquage de l’information

<Décrire le processus de marquage des informations>

* + - 1. Manipulation des actifs

<Décrire le processus de manipulation des actifs et d’utilisation correcte des actifs.>

* + - 1. Restitution des actifs

<Décrire le processus de restitution des actifs.>

### Manipulation des supports

* + - 1. Gestion des supports amovibles

<Décrire le processus de gestion des supports amovibles>

* + - 1. Mise au rebus des supports

<Décrire le processus de mise au rebus des supports>

* + - 1. Transfert physique des supports

<Décrire le processus de transfert des supports>

## Contrôle d’accès

### Exigences métier en matière de contrôle d’accès

* + - 1. Politique de contrôle d’accès

<Décrire le processus de contrôle d’accès>

* + - 1. Accès au réseau et aux services en réseau

<Décrire le processus d’accès au réseau>

### Gestion de l’accès utilisateur

* + - 1. Enregistrement et désinscription des utilisateurs

<Décrire le processus de mouvement du personnel et de gestion du cycle de vie des utilisateurs>

* + - 1. Maitrise de la gestion des accès utilisateurs

<Décrire le processus de mouvement du personnel>

* + - 1. Gestion des privilèges d’accès

<Décrire le processus de gestion des privilèges d’accès>

* + - 1. Gestion des informations secrètes d’authentification des utilisateurs

<Décrire la procédure de gestion des informations secrètes>

* + - 1. Revue des droits d’accès utilisateur

<Indiquer la procédure et la périodicité de la revue des droits>

### Responsabilités des utilisateurs

Chaque membre du personnel est responsable de protéger la confidentialité des éléments d’authentification (mot de passe, certificat, carte à puce, ...) qu’il détient pour se connecter aux équipements et services. Ils ne doivent être ni écrits, ni partagés. Ils ne doivent jamais être communiqués à d’autres personnes.

En cas de suspicion de compromission ou de vol, le personnel applique la procédure appropriée pour faire désactiver son compte ou renouveler les éléments d’authentification.

Chaque membre du personnel est responsable de la gestion des actifs qu’il détient et chacun doit protéger :

* Son poste de travail contre le vol à l’aide d’un câble antivol et en le conservant sous son contrôle lorsqu’il l’emporte à l’extérieur des locaux ;
* L’accès à sa session de travail en la verrouillant en cas d’absence même passagère et en effectuant des sauvegardes régulières du travail en cours ;
* Les données à l’aide de l’utilisation d’un filtre de confidentialité lorsque l’environnement et les données consultées l’exige ;
* Les informations identifiées comme sensibles, qu’elles soient numériques, au format papier ou orales, en appliquant les règles de protection associées.

<Indiquer su une politique s’applique et les éventuelles mesures associées aux responsabilités des utilisateurs>

### Contrôle de l’accès au système et à l’information

* + - 1. Restriction d’accès à l’information

<A compléter>

* + - 1. Sécuriser les procédures de connexion
         1. Accès aux serveurs de production

<A compléter>

* + - * 1. Administration des Serveurs

<A compléter>

* + - * 1. Administration des équipements réseau

<A compléter>

* + - * 1. Administration des équipements de sécurité

<A compléter>

* + - * 1. Accès aux machines de développement, test et intégration

<A compléter>

* + - * 1. Contrôles d’accès sur les applications

<A compléter>

* + - 1. Système de gestion des mots de passe

<A compléter>

* + - 1. Utilisation de programmes utilitaires à privilèges

<A compléter>

* + - 1. Contrôle d’accès au code source des programme

<A compléter>

## Cryptographie

### Politique d’utilisation des mesures cryptographiques

<Décrire la politique d’utilisation des mesures cryptographiques>

### Gestion des clés

<Décrire la procédure de gestion des clés>

## Sécurité physique et environnementale

### Zones sécurisées

* + - 1. Périmètre physique de sécurité

<A compléter>

* + - 1. Contrôle physique des accès

<A compléter>

* + - 1. Sécurisation des bureaux, des salles et des équipements

<A compléter>

* + - 1. Protection contre les menaces extérieures et environnementales

<A compléter>

* + - 1. Travail dans les zones sécurisées

<A compléter>

* + - 1. Zones de livraison et de chargement

<A compléter>

### Matériels

* + - 1. Emplacement et protection des matériels

<A compléter>

* + - 1. Service généraux

<A compléter>

* + - 1. Sécurité du câblage

<A compléter>

* + - 1. Maintenance des matériels

<A compléter>

* + - 1. Sortie des actifs

<A compléter>

* + - 1. Sécurité du matériel et des actifs hors des locaux

<A compléter>

* + - 1. Mise au rebut ou recyclage sécurisé du matériel

<A compléter>

* + - 1. Matériel utilisateur laissé sans surveillance

<A compléter>

* + - 1. Politique du bureau propre et de l’écran vide

<A compléter>

## Sécurité liée à l’exploitation

### Procédures et responsabilités liées à l’exploitation

* + - 1. Procédures d’exploitation documentées

<Décrire – ou indiquer la référence des documents correspondants – la ou les procédures d’exploitation (livraison de logiciels, exploitation du système, traitement des incidents, etc.)>

* + - 1. Gestion des changements

<Décrire la gestion des changements et les contrôles associés>

* + - 1. Dimensionnement

<Décrire le dimensionnement des machines, tolérance aux pannes et anticipation de pénurie de ressources>

* + - 1. Séparation des environnements de développement, de tests et d’exploitation

<Décrire les différents environnements ainsi que les niveaux de séparation et mesures associées>

### Protection contre les logiciels malveillants

* + - 1. Mesures générales

<A compléter>

* + - 1. Protection du poste de travail

<A compléter>

* + - 1. Protection des serveurs

<A compléter>

### Sauvegarde

Une procédure de sauvegarde régulière des données est une précaution indispensable pour se protéger contre les défaillances matérielles ou logicielles lourdes et contre les erreurs de manipulation.

Certains problèmes ne se manifestent pas toujours immédiatement. C’est pourquoi la sauvegarde doit être complétée par un archivage. De cette façon, en fonction de la nature du problème, il est possible de revenir à un état antérieur du système, complètement intègre et homogène.

<Décrire tout le processus de sauvegarde et d’archivage>

### Journalisation et surveillance

* + - 1. Journalisation des événements

Une politique opérationnelle de journalisation décrit l’ensemble des journaux d’évènement collectés.

Ces journaux enregistrent notamment les activités des utilisateurs, les exceptions, les défaillances et les événements liés à la sécurité. Ils contiennent notamment en fonction de l’activité les informations suivantes :

* Les identifiants utilisateurs ;
* Les activités du système ;
* La date, l’heure et les détails relatifs aux événements significatifs, par exemple les ouvertures et fermetures de session (application et système) ;
* Les actions significatives de l’utilisateur (notamment celle dont on doit éventuellement prouver l’imputabilité) ;
* L’identité ou l’emplacement du terminal si possible et l’identifiant du système ;
* Les enregistrements des tentatives d’accès au système, réussies et avortées ;
* Les enregistrements des tentatives d’accès aux données et autres ressources, réussies ou avortées ;
* Les exceptions et défaillances de l’application ou du système ;
* Les évènements liés à la sécurité.

<Décrire les règles régissant la gestion des traces>

* + - 1. Protection de l’information journalisée

<Décrire les mesures de protection de l’information journalisée>

* + - 1. Journaux administrateurs et opérateurs

<Décrire les mesures spécifiques des accès administrateurs et opérateurs>

* + - 1. Synchronisation des horloges

Afin de garantir un horodatage fiable des traces d’audit, et des données sensibles, une base de temps fiable est mise en œuvre afin de rendre un service de synchronisation des horloges systèmes des équipements. Le service de synchronisation est basé sur le protocole standardisé NTP (Network Time Protocol) qui permet de compenser les dérives horaires.

<Décrire les processus mis en œuvre pour la synchronisation des horloges, les références de temps utilisés, etc.>

### Maitrise des logiciels en exploitation

* + - 1. Installation de logiciels sur des systèmes en exploitation

<Décrire Le processus de réalisation des opérations de modifications et de changements relatifs à la maintenance et la mise à jour des équipements, systèmes et logiciels, ainsi qu’à la mise en production des nouvelles versions des applications>

### Gestion des vulnérabilités techniques

* + - 1. Gestion des vulnérabilités techniques éditeur

<Décrire le processus de veille et collecte des alertes>

* + - 1. Processus de traitement des vulnérabilités

<Décrire le processus de traitement des vulnérabilités, ainsi que le plan d’action adapté aux vulnérabilités critiques, majeures et mineures.>

* + - 1. Restrictions relatives à l’installation de logiciels

<Décrire la procédure relative aux restrictions d’installation de logiciels>

### Protection contre les Dénis de service

<Décrire les mesures et mécanismes mis en place afin de lutter contre des attaques de type DDoS>

## Sécurité des communications

### Cloisonnement et filtrage

<Décrire les accès entre les réseaux publics et le réseau d’entreprise, les flux de communication entre matériels, les protocoles autorisés, etc.>

### Gestion de la sécurité du réseau

* + - 1. Protection des flux

<Décrire les mécanismes de protection des flux>

* + - 1. Cloisonnement par niveau de sécurité

<Indiquer si un cloisonnement est mis en place (séparation des réseaux et séparation des applications)>

* + - 1. Plan d’adressage

<Indiquer si un plan d’adressage a été mis en place (adresses routables, translation des adresses, etc.)>

### Echange de l’information

* + - 1. Procédure de transfert de l’information

<Décrire comment la gestion des accès à l’information est réalisée. Préciser les principes qui sont appliqués pour protéger les informations gérées par le Prestataire, et notamment : la classification de l’information, le marquage de l’information et les mesures de protection de l’information>

* + - 1. Accords en matière de transfert d’information

<Décrire comment est géré le transfert de l’information du Client>

* + - 1. Messagerie électronique

<Préciser comment l’information du Client ou liée au projet du Cleint transitant par la messagerie électronique est protégée>

* + - 1. Engagements de confidentialité ou de non-divulgation

<Décrire les exigences en matière d’engagements de confidentialité ou de non-divulgation>

## Acquisition, développement et maintenance des systèmes d’information

### Exigences de sécurité applicables aux systèmes d’information

* + - 1. Analyse et spécification des exigences de sécurité de l’information

<Préciser, entre autre, les exigences de sécurité, de disponibilité, de conformité métier et réglementaire>

* + - 1. Sécurisation des services d’application sur les réseaux publics

<Indiquer les mécanismes mis en œuvre pour sécuriser les flux et données transitant sur les réseaux publics>

### Sécurité des processus de développement sécurisé

* + - 1. Politique de développement sécurisé

<Le Prestataire décrit :

* Les mesures prises pour le développement sécurisé ;
* La méthodologie adoptée pour assurer ce développement sécurisé ;
* Les spécifications de sécurité ;
* Les lignes directrices de codage de sécurité ;
* Les lignes directrices de configuration sécurisée ;
* Les guides et procédures de sécurité ;
* Les outils de contrôle de code ;
* Les revues de code>
  + - 1. Procédures de contrôles des changements apportés au système

<Décrire la gestion des changements et les contrôles associés>

* + - 1. Revue technique des applications après changement apporté à la plateforme

<Décrire les procédures de déploiement en production et les procédures de test de validation post mise en production>

* + - 1. Principes d’ingénierie de la sécurité des systèmes

<Décrire les principes d’ingénierie de la sécurité des systèmes et la documentation associée. Préciser les moyens qui concourent à assurer que les livrables produits dans le cadre de la prestation respectent les exigences de sécurité >

* + - 1. Environnement de développement sécurisé

<Décrire les principes de sécurisation appliqués aux environnements de développements et d’intégration>

* + - 1. Développement externalisé

<Décrire les exigences contractuelles et techniques en cas de sous-traitance des développements>

* + - 1. Phase de test de la sécurité du système

<Décrire la ou les procédures permettant de tester la sécurité du système>

* + - 1. Audit du code

<Le Prestataire précise les clauses permettant au Client de réaliser des audits de code sur les applications qui relèvent de leur périmètre de responsabilité. Le délai de préavis du Client pour mener ces audits doit être de quinze (15) jours ouvrés maximum.>

### Protection des Données

* + - 1. Protection des données de test et de recette

<Indiquer comment sont protéger les données de test et de recette>

* + - 1. Protection des données de production

<Indiquer comment sont protégées les données de production. Indiquer la méthode d’anonymisation retenue>

## Relations avec les fournisseurs

### Sécurité dans les relations avec les fournisseurs

* + - 1. Politique de sécurité de l’information dans les relations avec les fournisseurs

<Décrire la politique générale de sécurité de l’information dans les relations avec les fournisseurs. Lister les fournisseurs dans le périmètre du projet>

* + - 1. La sécurité dans les accords conclus avec les fournisseurs

Les exigences liées à la sécurité de l'information notamment sont gérées contractuellement avec les fournisseurs. Ceux-ci, en particulier s'ils interviennent dans le cadre de projets liées à de la donnée personnelle, sensible ou de santé doivent garantir contractuellement le respect : du RGPD, des droits de propriétés intellectuelles, des standards de sécurité, de la sécurité de l'information et de toutes les normes applicables aux projets cibles de leur intervention.

Les règles du Prestataire sur la classification de l’information est diffusée à l’ensemble de ses fournisseurs. <Compléter si nécessaire>

* + - 1. Chaine d’approvisionnement informatique

Le Prestataire intègre a minima dans les contrats de ses fournisseurs critiques (susceptible d’accéder aux données, même chiffrées) les exigences suivantes :

* <Lister les exigences demandées>

Si cela n’est pas possible, le Prestataire gère le risque après l’avoir identifié en élaborant un Plan de Traitement du Risque.

### Gestion de la prestation du service

* + - 1. Surveillance et revue des services des fournisseurs

<Indiquer comment sur suivis les fournisseurs du Prestataire>

* + - 1. Gestion des changements apportés dans les services des fournisseurs

<Décrire comment sont gérés les changements entre le Prestataire et ses fournisseurs>

## Gestion des incidents liés à la sécurité de l’information

### Gestions des incidents liés à la sécurité de l’information et amélioration

La typologie des incidents de sécurité est ainsi établie. Cette liste n’est pas exhaustive est pourra être compléter par le prestataire.

* Incidents de sécurité touchant la sécurité physique :
  + accès ou tentative d’accès non autorisé aux locaux ;
  + détérioration volontaire ou non d’un équipement de sécurité ;
  + perte ou vol d’un équipement ou support de stockage (électronique ou papier) pouvant contenir des données sensibles.
* Incidents de sécurité touchant la sécurité logique :
  + accès ou tentatives d’accès non autorisé à une information ou un système d’information (vol de compte sur un système, intrusion, écoute passive du réseau, etc.) ;
  + divulgation malveillante ou involontaire et sans autorisation d’une information classée « interne », « confidentielle » ou « secrète » ou d’une donnée sensible (mot de passe, clé de chiffrement …) ;
  + altération (modification non autorisée ou destruction) d’une information ou d’un système d’information (configuration, logiciel, etc.) ;
  + code malveillant ;
  + déni de service.

Cette typologie est indépendante de l’origine de l’incident. Il peut s’agir :

* Soit d’une personne du Prestataire ou d’une personne externe commettant un acte volontaire ou accidentel ;
* Soit d’un phénomène naturel ou d’un évènement lié à une activité humaine.
  + - 1. Responsabilités et procédure

<Décrire les responsabilités et les procédures des gestions des incidents>

* + - 1. Signalement des événements liés à la sécurité de l’information

Tout évènement lié à la sécurité de l’information fait l’objet d’une communication, dans les plus brefs délais, aux acteurs concernés (responsables hiérarchiques, équipes concernées) du Client et du Prestataire.

<Décrire le processus de déclaration d’incident. Il est possible de faire référence à un document externe.>

* + - 1. Signalement des failles liées à la sécurité de l’information

<Décrire le processus de failles>

* + - 1. Appréciation des événements liés à la sécurité de l’information et prise de décision

Un incident de sécurité est différencié d’un incident classique selon les modalités suivantes :

* Un incident de sécurité est un événement ou une série d’événements indésirables ou inattendus liés à la sécurité de l’information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l’organisation et de menacer la sécurité de l’information.
* Un évènement de sécurité est l’occurrence identifiée de l’état d’un service, d’un système ou d’un réseau indiquant une faille possible dans la politique de sécurité de l’information ou un échec des mesures de sécurité.
* Une faille de sécurité est une vulnérabilité avérée dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité et l’intégrité des données qu’il contient.

<Décrire le processus de classement des événements liés à la sécurité.>

* + - 1. Réponse aux incidents liés à la sécurité de l’information

<Décrire la procédure de gestion des incidents de sécurité affectant un des systèmes d’information (notamment la qualification des incidents, l’escalade des incidents, la procédure en cas de déclaration de crise et le processus général de traitement des incidents >

* + - 1. Tirer des enseignements des incidents liés à la sécurité de l’information

<Décrire la procédure de RETEX>

* + - 1. Recueil de preuves

<Indiquer la procédure de recueil de preuve>

## Organisation et mise œuvre de la continuité de la sécurité de l’information

### Continuité de la sécurité de l’information

* + - 1. Organisation de la continuité de la sécurité de l’information

<Décrire l’organisation mise en place dans le cadre d’un PCA>

* + - 1. Mise en œuvre de la continuité de la sécurité de l’information

<Décrire la mise en œuvre d’un PCA>

* + - 1. Revue du plan de continuité d’activité

<Décrire la procédure de revue du PCA>

### Redondances

* + - 1. Redondance des matériels

<Décrire les mécanismes mis en place de redondance des matériels>

* + - 1. Redondance des réseaux

<Décrire les mécanismes mis en place de redondance des réseaux (internet, Ethernet, etc.>

## Conformité

### Conformité aux exigences légales et réglementaires

* + - 1. Identification de la législation et des exigences contractuelles applicables

<Indiquer les principaux textes/référentiels applicables pour la prestation>

* + - 1. Droits de propriété intellectuelle

<Indiquer les processus de vérification de conformité (procédure d’achat de matériel et de licences de logiciels, prestation intellectuelle)>

* + - 1. Protection des enregistrements

<Indiquer les mécanismes de protection des enregistrements>

* + - 1. Protection de la vie privée et des données à caractère personnel

<Description des mécanismes de protection de la vie privée et des données à caractère personnel>

Le Prestataire s’engage à :

* Sensibiliser et former périodiquement ses collaborateurs à la protection des données personnelles confiées par le Client ;
* Conseiller par écrit le Client en tant que sous-traitant quant à la mise en œuvre du RGPD ;
* Fournir au Client les informations techniques relevant du périmètre du Prestataire.

Le Client, en tant que Responsable de traitement, s’engage à donner par écrit les instructions de traitement des données personnelles au Prestataire.

* + - 1. Réglementation relative aux mesures cryptographiques

Le Prestataire s’engage à mettre en œuvre des mesures cryptographiques conformément aux accords, lois et règlementations applicables.

<Indiquer les recommandations suivies et processus d’exception>

### Revue de la sécurité de l’information

* + - 1. Revue indépendante de la sécurité de l’information

<Décrire le programme d’audit>

* + - 1. Conformité avec les politiques et normes de sécurité

<Décrire les revues de conformité effectuées et leurs périodicités>

* + - 1. Vérification de la conformité technique

<Décrire la procédure de vérification de la conformité technique>

## Homologation

L’homologation est une démarche de maîtrise des risques sur le SI. L’homologation est l’attestation formelle que les besoins de sécurité ont été identifiés et traités de manière à ce que les risques résiduels soient maîtrisés et acceptables

### Homologation du Prestataire

Le Prestataire fournira au Client les décisions d’homologation déjà prononcées sur les systèmes d’information impliqués dans le cadre du projet, ainsi que la liste des risques résiduels issus des analyses de risque correspondantes.

### Dossier de sécurité

* + - 1. Constitution du dossier de sécurité

Le Prestataire établit pour chaque projet, un dossier de sécurité présentant les données et leurs traitements, les mesures générales et particulières de sécurité, les moyens de protection associés ainsi que les moyens et techniques concourant au fonctionnement du système d’information. Il recense les vulnérabilités résiduelles.

Le Prestataire maintient à jour les éléments constitutifs du dossier de sécurité. Les pièces constitutives du dossier de sécurité sont soumises au Client pour validation.

<Décrire le processus du maintien à jour du dossier>

* + - 1. Livrables

Les documents constitutifs du dossier de sécurité sont :

* <Lister les pièces attendues dans le cadre de cette prestation>

Tout document du dossier de sécurité doit être expressément validé par le RSSI du Client afin d’être considéré comme finalisé. Celle validation peut être considérée comme tacite au-delà d’une période de 60 jours à partir de la date de livraison au RSSI du Client.

* + - * 1. Analyse de risque

Le Prestataire doit rédiger (avec le concours du Client) et maintenir à jour l’analyse de risques du système en vue d’identifier les risques auxquels l'application est confrontée. Cette action devrait identifier les principaux risques pesant sur les biens et fonctions essentiels fournis par l'application, ainsi que les mesures à mettre en œuvre pour diminuer la vraisemblance des risques.

<Décrire la méthodologie d’analyse de risque utilisée.

Le Prestataire inclut dans cette analyse de risque un volet sur la sécurité des données à caractère personnel et l’impact sur la vie privée de la personne concernée, en cas de compromission ou altération de ces dernières. >.

* + - * 1. Dossier d’Architecture Technique

<Indiquer les sujets traités par le DAT, inclure des schémas. Il est possible de faire référence à un document externe.

Ce DAT inclut une cartographie des SI du Client. Le Prestataire y détaille les parties techniques. Il est possible de faire référence à un document externe.>

* + - * 1. Procédure d’Exploitation de la Sécurité

<Indiquer les thématiques couvertes par la ou les PES. Il est possible de faire référence à ou plusieurs documents externes.>

* + - * 1. Maintien en Condition de Sécurité

<Préciser les différents outils, procédures, mécanismes mis en œuvre afin d’assurer un MCS pérenne dans le temps de la prestation. Le Prestataire précise aussi comment est réalisé le suivi :

* Des vulnérabilités découvertes et la gestion des correctifs de sécurité ;
* Des alertes ou attaques.

Il est possible de faire référence à ou plusieurs documents externes.>

* + - * 1. Fiches réflexes

<Indiquer les thématiques des fiches réflexes qui seront créées durant la prestation. Il est possible de faire référence à ou plusieurs documents externes.>

## Analyse de risque stratégique

[Si une analyse de risque stratégique est jointe au marché, le Prestataire sera en charge de réaliser l’analyse de risque correspondante. Pour cela le Prestataire détaillera sa réponse en précisant :

* La méthodologie qu’il emploiera pour la réalisation de cette analyse ;
* Le nombre de réunions / d’ateliers prévus ;
* Le profil des participants à chaque réunion ;
* Les livrables.]

# Matrice de couverture des exigences de sécurité

Le Prestataire indique dans le tableau suivant le paragraphe du PAS qui répond à chaque exigence exprimée par le Client (cf. chapitre 7).

|  |  |
| --- | --- |
| Exigence de sécurité du Client | Prise en compte dans le présent PAS |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

<Le Prestataire précise les clauses permettant au Client de réaliser des audits de conformité aux exigences de sécurité (audit de conformité au PAS, …).

Le délai de préavis du Client pour mener ces audits doit être de quinze (15) jours ouvrés maximum.>

# Annexe

## Glossaire

|  |  |
| --- | --- |
| ANSSI | Agence nationale de la sécurité des systèmes d’information |
| AQSSI | Autorité Qualifiée en Sécurité des Systèmes d’Information |
| C2MI | Centre de Cyberdéfense du Ministère de l’Intérieur |
| Confidentialité | Propriété garantissant que l'accès à une information ou à un traitement est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés. |
| CNIL | Commission nationale de l’informatique et des libertés |
| Disponibilité | Propriété d’une information ou d’un traitement d’être utilisable à la demande par une personne ou par un système. |
| Incident SSI | Évènement lié au système d’information, pertinent du point de vue SSI, par lequel la PSSI du système d'information est violée ou non respectée, pouvant conduire à la survenance d’un sinistre SSI. |
| Intégrité | Propriété garantissant qu’une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée. |
| MI | Ministère de l’Intérieur |
| PAS | Plan d’Assurance Sécurité |
| PSSIE | Politique de Sécurité des Systèmes d’Information de l’Etat |
| PSSI-MI | Politique de Sécurité des Systèmes d’Information pour le Ministère de l’Intérieur |
| RGPD | Règlements Général sur le Protection des Données |
| RSSI | Responsable de la Sécurité des Systèmes d’Information |
| SHFD | Service du Haut Fonctionnaire de Défense |
| SIE MI | Système d’Information Essentiel du ministère de l’Intérieur |
| SI | Système d’information |
| Sinistre SSI | Incident SSI dont la survenance cause des dommages au système d'information. |
| SSI | Sécurité des systèmes d’information |
| Traçabilité | Aptitude à conserver et retrouver les traces de l’état et des mouvements de l’information. Cette propriété est particulièrement utilisée dans le cadre d’incident SSI. |

## Conformité PSSI-MI

Le Prestataire a l’obligation de réaliser une conformité à la PSSI du ministère de l’intérieur (PSSI-MI)[[1]](#footnote-1). Les exigences seront notées :

* N/A Non applicable
* 0 N’est pas appliqué
* 1 Est partiellement appliqué mais l’écart est important
* 2 Est partiellement appliqué et l’écart est faible
* 3 Est complètement appliqué

Toute exigence n’ayant pas une note à 3 devra obligatoire être dûment justifiée.

|  |  |  |
| --- | --- | --- |
| Domaine | Référence | Note |
| 1. Politique, organisation, gouvernance | ORG-SSI : organisation SSI |  |
| ORG-ACT-SSI : identification des acteurs SSI |  |
| ORG-RSSI : désignation du responsable SSI |  |
| ORG-RESP : formalisation des responsabilités. |  |
| ORG-TIERS : gestion contractuelle des tiers |  |
| ORG-PIL-PSSI : définition et pilotage de la PSSI |  |
| ORG-APP-INSTR : application de l’instruction dans l’entité |  |
| ORG-APP-DOCS : formalisation de documents d’application |  |
| 2. Ressources humaines | RH-SSI : charte d’application SSI |  |
| RH-MOTIV : choix et sensibilisation des personnes tenant les postes clés de la SSI. |  |
| RH-CONF : personnels de confiance. |  |
| RH-UTIL : sensibilisation des utilisateurs des systèmes d’information. |  |
| RH-MOUV : gestion des arrivées, des mutations et des départs. |  |
| RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, …) |  |
| 3. Gestion des biens | GDB-INVENT : inventaire des ressources informatiques |  |
| GDB-CARTO : cartographie. |  |
| GDB-QUALIF-SENSI : qualification des informations |  |
| GDB-PROT-IS : protection des informations |  |
| 4. Intégration de la SSI | INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d’information |  |
| INT-SSI : intégration de la sécurité dans les projets |  |
| INT-QUOT-SSI : mise en œuvre au quotidien de la SSI |  |
| INT-TDB : créer un tableau de bord SSI |  |
| INT-AQ-PSL : acquisition de produits et services de confiance |  |
| INT-PRES-CS : clauses de sécurité |  |
| INT-PRES-CNTRL : suivi et contrôle des prestations fournies |  |
| INT-REX-AR : analyse de risques |  |
| INT-REX-HB : hébergement. |  |
| INT-REX-HS : hébergement et clauses de sécurité |  |
| 5. Sécurité physique | PHY-ZONES : découpage des sites en zones de sécurité |  |
| PHY-PUBL : accès réseau en zone d’accueil du public |  |
| PHY-SENS : protection des informations sensibles au sein des zones d’accueil |  |
| PHY-TECH : sécurité physique des locaux techniques |  |
| PHY-TELECOM : protection des câbles électriques et de télécommunications |  |
| PHY-CTRL : contrôles anti-piégeages |  |
| PHY-CI-LOC : découpage des locaux en zones de sécurité |  |
| PHY-CI-HEBERG : convention de service en cas d’hébergement tiers |  |
| PHY-CI-CTRLACC : contrôle d’accès physique |  |
| PHY-CI-MOYENS : délivrance des moyens d’accès physique. |  |
| PHY-CI-TRACE : traçabilité des accès |  |
| PHY-CI-ENERGIE : local énergie |  |
| PHY-CI-CLIM : climatisation |  |
| PHY-CI-INC : lutte contre l’incendie |  |
| PHY\_CI-EAU : lutte contre les voies d’eau |  |
| PHY-SI-SUR : sécurisation du SI de sûreté |  |
| 6. Sécurité des réseaux | RES-MAITRISE : systèmes autorisés sur le réseau |  |
| RES-INTERCO : interconnexion avec des réseaux externes |  |
| RES-ENTSOR : mettre en place un filtrage réseau pour les flux sortants et entrants |  |
| RES-PROT : protection des informations |  |
| RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes |  |
| RES-INTERCOGEO : interconnexion des sites géographiques locaux d’une entité |  |
| RES-RESS : cloisonnement des ressources en cas de partage de locaux |  |
| RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité. |  |
| RES-SSFIL : mise en place de réseaux sans fil. |  |
| RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses. |  |
| RES-ROUTDYN : surveiller les annonces de routage. |  |
| RES-ROUTDYN-IGP : configurer le protocole IGP de manière sécurisée. |  |
| RES-ROUTDYN-EGP : sécuriser les sessions EGP. |  |
| RES-SECRET : modifier systématiquement les éléments d’authentification par défaut des équipements et services. |  |
| RES-DURCI : durcir les configurations des équipements de réseaux |  |
| RES-CARTO : élaborer les documents d’architecture technique et fonctionnelle. |  |
| 7. Architecture des SI | ARCHI-HEBERG : principes d’architecture de la zone d’hébergement |  |
| ARCHI-STOCKCI : architecture de stockage et de sauvegarde |  |
| ARCHI-PASS : passerelle Internet |  |
| 8. Exploitation des SI | EXP-PROT-INF : protection des informations sensibles en confidentialité et en intégrité |  |
| EXP-TRAC : traçabilité des interventions sur le système |  |
| EXP-CONFIG : configuration des ressources informatiques |  |
| EXP-DOC-CONFIG : documentation des configurations |  |
| EXP-ID-AUTH : identification, authentification et contrôle d’accès logique |  |
| EXP-DROITS : droits d’accès aux ressources |  |
| EXP-PROFILS : gestion des profils d’accès aux applications |  |
| EXP-PROC-AUTH : autorisations d’accès des utilisateurs |  |
| EXP-REVUE-AUTH : revue des autorisations d’accès |  |
| EXP-CONF-AUTH : confidentialité des informations d’authentification |  |
| EXP-GEST-PASS : gestion des mots de passe |  |
| EXP-INIT-PASS : initialisation des mots de passe |  |
| EXP-POL-PASS : politiques de mots de passe |  |
| EXP-CERTIFS : utilisation de certificats électroniques |  |
| EXP-QUAL-PASS : contrôle systématique de la qualité des mots de passe. |  |
| EXP-SEQ-ADMIN : séquestre des authentifiants « administrateur » |  |
| EXP-POL-ADMIN : politique de mots de passe « administrateurs ». |  |
| EXP-DEP-ADMIN : gestion du départ d’un administrateur des SI |  |
| EXP-RESTR-DROITS : restriction des droits |  |
| EXP-PROT-ADMIN : protection des accès aux outils d’administration |  |
| EXP-HABILIT-ADMIN : habilitation des administrateurs |  |
| EXP-GEST-ADMIN : gestion des actions d’administration |  |
| EXP-SEC-FLUXADMIN : sécurisation des flux d’administration |  |
| EXP-CENTRAL : centraliser la gestion du système d’information |  |
| EXP-SECX-DIST : sécurisation des outils de prise de main à distance |  |
| EXP-DOM-POL : définir une politique de gestion des comptes du domaine |  |
| EXP-DOM-PASS : configurer la stratégie des mots de passe des domaines |  |
| EXP-DOM-NOMENCLAT : définir et appliquer une nomenclature des comptes du domaine |  |
| EXP-DOM-RESTADMIN : restreindre au maximum l’appartenance aux groupes d’administration du domaine. |  |
| EXP-DOM-SERV : maîtriser l’utilisation des comptes de service |  |
| EXP-DOM-LIMITSERV : limiter les droits des comptes de service. |  |
| EXP-DOM-OBSOLET : désactiver les comptes du domaine obsolètes |  |
| EXP-DOM-ADMINLOC : améliorer la gestion des comptes d’administrateur locaux |  |
| EXP-MAINT-EXT : maintenance externe |  |
| EXP-MIS-REB : mise au rebut |  |
| EXP-PROT-MALV : protection contre les codes malveillants. |  |
| EXP-GES-ANTIVIR : gestion des événements de sécurité de l’antivirus |  |
| EXP-MAJ-ANTIVIR : mise à jour de la base de signatures |  |
| EXP-NAVIG : configuration du navigateur Internet |  |
| EXP-POL-COR : définir et mettre en œuvre une politique de suivi et d’application des correctifs de sécurité |  |
| EXP-COR-SEC : déploiement des correctifs de sécurité |  |
| EXP-OBSOLET : assurer la migration des systèmes obsolètes |  |
| EXP-ISOL : isoler les systèmes obsolètes restants |  |
| EXP-JOUR-SUR : journalisation des alertes |  |
| EXP-POL-JOUR : définir et mettre en œuvre une politique de gestion et d’analyse des journaux de traces |  |
| EXP-CONS-JOUR : conservation des journaux. |  |
| EXP-GES-DYN : gestion dynamique de la sécurité |  |
| EXP-MAIT-MAT : maîtrise des matériels. |  |
| EXP-PROT-VOL : rappel des mesures de protection contre le vol |  |
| EXP-DECLAR-VOL : déclarer les pertes et vols |  |
| EXP-REAFFECT : réaffectation de matériels informatiques |  |
| EXP-NOMAD-SENS : déclaration des équipements nomades aptes à traiter des informations sensibles |  |
| EXP-ACC-DIST : accès à distance au système d’information de l’organisme |  |
| EXP-IMP-SENS : impression des informations sensibles. |  |
| EXP-IMP-2 : sécurité des imprimantes et copieurs multifonctions |  |
| EXP-CI-OS : systèmes d’exploitation |  |
| EXP-CI-LTP : logiciels en Tiers Présentation |  |
| EXP-CI-LTA : logiciels en Tiers Application |  |
| EXP-CI-LTD : logiciels en Tiers Données |  |
| EXP-CI-PROTFIC : passerelle d’échange de fichiers |  |
| EXP-CI-MESSTECH : messagerie technique |  |
| EXP-CI-FILT : filtrage des flux applicatifs |  |
| EXP-CI-ADMIN : flux d’administration |  |
| EXP-CI-DNS : service de noms de domaine – DNS technique |  |
| EXP-CI-EFFAC : effacement de support. |  |
| EXP-CI-DESTR : destruction de support |  |
| EXP-CI-TRAC : traçabilité / imputabilité |  |
| EXP-CI-SUPERVIS : supervision |  |
| EXP-CI-AMOV : accès aux périphériques amovibles |  |
| EXP-CI-ACCRES : accès aux réseaux |  |
| EXP-CI-AUDIT : audit/contrôle |  |
| 9. Sécurité du poste de travail | PDT-GEST : fourniture et gestion des postes des travail |  |
| PDT-CONFIG : formalisation de la configuration des postes des travail |  |
| PDT-VEROUIL-FIXE : verrouillage de l’unité centrale des postes fixes |  |
| PDT-VEROUIL-PORT : verrouillage des postes portables |  |
| PDT-REAFFECT : réaffectation du poste de travail |  |
| PDT-PRIVIL : privilèges des utilisateurs sur les postes de travail |  |
| PDT-PRIV : utilisation des privilèges d’accès « administrateur » |  |
| PDT-ADM-LOCAL : gestion du compte « administrateur local ». |  |
| PDT-STOCK : stockage des informations |  |
| PDT-SAUV-LOC : sauvegarde / synchronisation des données locales |  |
| PDT-PART-FIC : partage de fichiers |  |
| PDT-SUPPR-PART : suppression des données sur les postes partagés |  |
| PDT-CHIFF-SENS : chiffrement des données sensibles |  |
| PDT-AMOV : fourniture de supports de stockage amovibles |  |
| PDT-NOMAD-ACCESS : accès à distance aux Systèmes d’Information de l’entité |  |
| PDT-NOMAD-PAREFEU : pare-feu local |  |
| PDT-NOMAD-STOCK : stockage local d’information sur les postes nomades |  |
| PDT-NOMAD-FILT : filtre de confidentialité |  |
| PDT-NOMAD-CONNEX : configuration des interfaces de connexion sans fil |  |
| PDT-NOMAD-DESACTIV : désactivation des interfaces de connexion sans fil |  |
| PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions. |  |
| PDT-MUL-SECNUM : sécurisation de la fonction de numérisation |  |
| PDT-TEL-MINIM: sécuriser la configuration des autocommutateurs |  |
| PDT-TEL-CODES : codes d’accès téléphoniques |  |
| PDT-TEL-DECT : limiter l’utilisation du DECT |  |
| PDT-CONF-VERIF : utiliser des outils de vérification automatique de la conformité |  |
| 10. Sécurité du développement des systèmes | DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux |  |
| DEV-SOUS-TRAIT : intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique |  |
| DEV-FUITES : limiter les fuites d’information |  |
| DEV-LOG-ADHER : réduire l’adhérence des applications à des produits ou technologies spécifiques |  |
| DEV-LOG-CRIT : instaurer des critères de développement sécurisé |  |
| DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel |  |
| DEV-LOG-WEB : améliorer la prise en compte de la sécurité dans les développements Web |  |
| DEV-LOG-PASS : calculer les empreintes de mots de passe de manière sécurisée |  |
| DEV-FILT-APPL : mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque |  |
| 11. Traitement des incidents | TI-OPS-SSI : chaînes opérationnelles SSI |  |
| TI-MOB : mobilisation en cas d’alerte |  |
| TI-QUAL-TRAIT : qualification et traitement des incidents |  |
| TI-INC-REM : remontée des incidents |  |
| 12. Continuité d’activité | PCA-MINIS : définition du plan ministériel de continuité d’activité des Systèmes d’Information. |  |
| PCA-LOCAL : définition du plan local de continuité d’activité des systèmes d’information |  |
| PCA-SUIVILOCAL : suivi de la mise en œuvre du plan de continuité d’activité local des Systèmes d’Information (PCA des SI). |  |
| PCA-PROC : mise en œuvre des dispositifs techniques et des procédures opérationnelles |  |
| PCA-SAUVE : protection de la disponibilité des sauvegardes |  |
| PCA-PROT : protection de la confidentialité des sauvegardes |  |
| PCA-EXERC : exercice régulier du plan local de continuité d’activité des systèmes d’information. |  |
| PCA-MISAJOUR : mise à jour du plan local de continuité d’activité des systèmes d’information |  |
| 13. Conformité, audit, inspection, contrôle | CONTR-SSI : contrôles locaux |  |
| CONTR-BILAN-SSI : bilan annuel |  |

1. Un fichier Excel ou Calc est fournis au Prestataire expliquant chaque exigence. [↑](#footnote-ref-1)