Plan d’Assurance Sécurité

Des Ministères Sociaux pour

TITULAIRE

Fourniture de prestations, de licences associées, d’assistance, de réalisation, de maintenance, de formation, et de support, à la mise en place de systèmes de bulles sécuritaires pour les projets actuels et à venir de la direction du numérique des ministères sociaux « DNUM »

(Bulles sécuritaires DNUM)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Prestation |  | | | |
| Titulaire |  | | | |
| Référence contrat | | Version | Date | Statut |
|  | | V0.0 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Suivi des modifications | | | |
| Version | Date | Auteur | Modifications |
| 1 | 17/11/2025 | Ministère/DNUM/BAFA | Version définitive |
|  |  |  |  |
|  |  |  |  |

Version 1 du 17/11/2025

Préambule

Ce document est un modèle type, ayant pour but de faciliter la rédaction d’un plan d’assurance sécurité pour l’externalisation d’activités ou d’hébergement.

Ce document doit faire partie du contrat passé avec le titulaire ; il est validé conjointement par le ministère et le titulaire, avant d'être annexé au contrat.

Lorsque plusieurs sites sont utilisés pour une même prestation, un seul PAS est à réaliser. Les particularités de chaque site seront formellement identifiées.

|  |
| --- |
| Les aspects contractuels liés à l’application ou au manquement de l’application du PAS sont à traiter dans les articles correspondants du contrat. Par ailleurs, les aspects relatifs au respect de la confidentialité sont également précisés dans le contrat, ainsi que dans les engagements de confidentialité éventuellement signés par les parties. |

|  |
| --- |
| Le PAS est spécifique à un titulaire. Si le projet sous-traite des activités à plusieurs titulaires, il devra mettre en œuvre plusieurs PAS. |

Avant-propos

Les informations, ainsi que les systèmes informatiques permettant de les traiter constituent une part essentielle du patrimoine des ministères chargés des affaires sociales, il et plus généralement de l’administration de l’Etat. Ces systèmes d’information (SI) sont exposés à de multiples menaces pouvant gravement porter atteinte au fonctionnement des structures et de l’Etat. Par ailleurs, l’exposition et la complexité des SI ne font que croître, du fait de besoins d’ouverture, de mutualisation, d’harmonisation, de valorisation et de flexibilité toujours plus importants.

Le présent document constitue le **plan d’assurance sécurité (PAS) des Ministères Sociaux** pour l’externalisation de ses systèmes d’information. Tout candidat à des prestations externalisées doit s’engager sur la sécurité telle qu’elle est décrite dans ce plan d’assurance sécurité type.

La rédaction de ce document a été réalisée en s’appuyant sur la Politique de sécurité du système d’information **des Ministères Sociaux**, ainsi que sur le guide « maitriser les risques de l’infogérance » de l’Agence Nationale de la Sécurité des Systèmes d’Information.

Le PAS s’inscrit dans l’organisation de la chaine SSI **des Ministères Sociaux** et est destiné à couvrir les risques liés à l’externalisation du SI. Il s’adresse aux candidats à l‘externalisation de prestations des systèmes d’information **des Ministères Sociaux** et vise à formaliser une zone de confiance homogène entre les deux entités.

Le PAS **des Ministères Sociaux** précise :

* Les exigences liées à la Sécurité des SI, et les objectifs à satisfaire par le titulaire pour atteindre un niveau de sécurité conforme aux enjeux **des Ministères Sociaux**.
* L’organisation de la sécurité et notamment les rôles et responsabilité, ainsi que l’articulation entre les différents acteurs en charge de la Sécurité du SI **des Ministères Sociaux**.
* Les mesures de sécurité de l’information qui doivent être prise en compte par le titulaire pour l’infogérance des systèmes d’information **des Ministères Sociaux**.

Tables des matières

[1. Objectifs et exigences de Sécurité SI des Ministères Sociaux 7](#_Toc206746651)

[1.1.1 Objectifs de sécurité 7](#_Toc206746652)

[2. Organisation de la sécurité pour l’ensemble de la prestation 7](#_Toc206746653)

[3. Documents applicables 8](#_Toc206746654)

[3.1.1 Documents de référence 8](#_Toc206746655)

[3.1.2 Procédures d’évolution du PAS 8](#_Toc206746656)

[3.1.3 Applicabilité du PAS 8](#_Toc206746657)

[4. Cadre général de la prestation 9](#_Toc206746658)

[4.1.1 Description fonctionnelle de la prestation 9](#_Toc206746659)

[4.1.2 Lieux d’exécution 9](#_Toc206746660)

[4.1.3 Description de l’architecture 10](#_Toc206746661)

[4.1.4 Ressources matérielles 10](#_Toc206746662)

[4.1.5 Ressources logicielles 10](#_Toc206746663)

[4.1.6 Accès distants 10](#_Toc206746664)

[4.1.7 Exigences de sécurité et mesures de protection 11](#_Toc206746665)

[5. Cadre juridique 12](#_Toc206746667)

[5.1.1 Respect des contraintes sur les données à caractère personnel 12](#_Toc206746668)

[5.1.2 Localisation géographique des services et des données 13](#_Toc206746669)

[5.1.3 Certifications du Titulaire 14](#_Toc206746670)

[5.1.4 Répercussion des clauses sur les sous-traitants 15](#_Toc206746671)

[6. Organisation de la sécurité 16](#_Toc206746672)

[6.1.1 Responsabilités et rôles sécurité 16](#_Toc206746673)

[6.1.2 Existence d'une politique de sécurité 17](#_Toc206746674)

[6.1.3 Pilotage de la SSI 18](#_Toc206746675)

[6.1.4 Détection, alerte et traitement des incidents de sécurité 19](#_Toc206746676)

[6.1.5 Gestion de crise sécurité 20](#_Toc206746677)

[6.1.6 Base de connaissances 21](#_Toc206746678)

[6.1.7 Engagement Individuel de Confidentialité (EIC) 22](#_Toc206746679)

[6.1.8 Sensibilisation des intervenants 23](#_Toc206746680)

[6.1.9 Sensibilisation du personnel à la sécurité 25](#_Toc206746681)

[7. Audits et contrôles de sécurité 26](#_Toc206746682)

[7.1.1 Autocontrôle de sécurité 26](#_Toc206746683)

[7.1.2 Contrôles de sécurité 27](#_Toc206746684)

[7.1.3 Contrôle des connexions distantes 28](#_Toc206746685)

[7.1.4 Test de conformité des logiciels 29](#_Toc206746686)

[7.1.5 Sécurité des outils et services 30](#_Toc206746687)

[7.1.6 Correction des écarts identifiés 31](#_Toc206746688)

[8. Sécurité des environnements 32](#_Toc206746689)

[8.1.1 Protection contre les programmes malveillants 32](#_Toc206746690)

[8.1.2 Suivi de la protection contre les programmes malveillants 33](#_Toc206746691)

[8.1.3 Correctifs de sécurité 34](#_Toc206746692)

[8.1.4 Suivi de l'application des correctifs de sécurité 35](#_Toc206746693)

[9. Sécurité des données 35](#_Toc206746694)

[9.1.1 Gestion des données 36](#_Toc206746695)

[9.1.2 Marquage des ressources techniques 37](#_Toc206746696)

[9.1.3 Cloisonnement des données du Ministère 38](#_Toc206746697)

[9.1.4 Sauvegarde de la base de données contenant les mots de passe 39](#_Toc206746698)

[10. Sécurité des accès logiques 40](#_Toc206746699)

[10.1.1 Identifiants du Titulaire 40](#_Toc206746700)

[10.1.2 Identifiants du Ministère 41](#_Toc206746701)

[10.1.3 Authentification du Titulaire en administration 42](#_Toc206746702)

[10.1.4 Authentification du Titulaire sur les actions d'administration 43](#_Toc206746703)

[10.1.5 Authentification des utilisateurs du Ministère, des prestataires et des intervenants du Titulaire 44](#_Toc206746704)

[10.1.6 Authentification des utilisateurs du Ministère et des intervenants du Titulaire 45](#_Toc206746705)

[10.1.7 Gestion des privilèges 46](#_Toc206746706)

[10.1.8 Revue et suivi des comptes du domaine de responsabilités du Titulaire 47](#_Toc206746707)

[10.1.9 Traçabilité des accès logiques 48](#_Toc206746708)

[10.1.10 Suivi des mécanismes de traçabilité des accès logiques 49](#_Toc206746709)

[10.1.11 Détection des anomalies de gestion des accès 49](#_Toc206746710)

[11. Sécurité réseau 51](#_Toc206746711)

[11.1.1 Politique de gestion des flux réseau 51](#_Toc206746712)

[11.1.2 Cartographie des flux 52](#_Toc206746713)

[11.1.3 Chiffrement des flux 53](#_Toc206746714)

[11.1.4 Chiffrement des échanges inter-sites 54](#_Toc206746715)

[11.1.5 Prévention contre les attaques externes 55](#_Toc206746716)

[11.1.6 Traçabilité des accès réseau 56](#_Toc206746717)

[11.1.7 Suivi des mécanismes de traçabilité des accès réseau 57](#_Toc206746718)

[12. Sécurité physique 58](#_Toc206746719)

[12.1.1 Contrôle des accès physiques aux locaux du Titulaire 58](#_Toc206746720)

[12.1.2 Respect des normes de sécurité physiques et environnementales 59](#_Toc206746721)

[12.1.3 Contrôle des accès physiques aux ressources techniques du Titulaire 60](#_Toc206746722)

[12.1.4 Protection contre le vol 61](#_Toc206746723)

[12.1.5 Protection des plateaux mutualisés 62](#_Toc206746724)

[13. Sécurité lors de la réversibilité 63](#_Toc206746725)

[13.1.1 Maintien de la sécurité durant la réversibilité ou transfert de la prestation 63](#_Toc206746726)

[13.1.2 Destruction des données en fin de prestation 64](#_Toc206746727)

[14. Métiers 65](#_Toc206746728)

[14.1.1 Dispositif de validation des modifications 65](#_Toc206746729)

[14.1.2 Sécurité des mises en production 66](#_Toc206746730)

[14.1.3 Règles de sécurité et d'exploitation 67](#_Toc206746731)

[14.1.4 Sources d'installations des logiciels 68](#_Toc206746732)

[14.1.5 Validité des licences 69](#_Toc206746733)

[14.1.6 Identification et traitement des vulnérabilités 70](#_Toc206746734)

[14.1.7 Phase de réversibilité en fin de contrat 71](#_Toc206746735)

[15. Annexes 72](#_Toc206746736)

[15.1 Annexe 1 : Documents sécurité liés à la prestation 72](#_Toc206746737)

[15.1.1 Suivi sécurité 72](#_Toc206746738)

[15.1.2 Organisation, processus et procédures sécurité 73](#_Toc206746739)

[15.2 Annexe 2 : Procédure XXXXX 74](#_Toc206746740)

[15.3 Annexe 3 : Politique XXXX 74](#_Toc206746741)

# Objectifs et exigences de Sécurité SI des Ministères Sociaux

## Objectifs de sécurité

Les objectifs de sécurité des systèmes d’information définis par **les Ministères Sociaux** sont :

* D’assurer la disponibilité des infrastructures nationales. L’accès aux applications et aux services critiques **des Ministères Sociaux** est tributaire des infrastructures nationales ;
* De sécuriser les applications et les serveurs nationaux ;
* De protéger les environnements et les informations sous toutes leurs formes.

Il est primordial que les mesures de sécurité mises en œuvre par le titulaire soit d’un niveau au moins égal à celui imposé dans la politique de sécurité **des Ministères Sociaux** défini dans le cadre du contrat. Si ces mesures se révèlent non conformes lors de la prise en charge par TITULAIRE, elles seront traitées dans le cadre du plan d’amélioration continu.

# Organisation de la sécurité pour l’ensemble de la prestation

La sécurité est assurée au Ministère par :

Les coordonnées du Ministère seront mises à jour lors du démarrage de la prestation.

* Le responsable Contractuel du contrat  : [A compléter]
* Le RSSI  : [A compléter]

La sécurité est assurée au titulaire par :

* Le responsable Contractuel du contrat : [A compléter]
* Le responsable Sécurité du contrat  : [A compléter]

L’ensemble des problématiques de sécurité seront présentées et suivies lors des points de suivi entre le responsable du contrat et le titulaire [A compléter]

Le RSSI du ministère a pouvoir de valider les décisions sur cette thématique.

Les deux parties prenantes ont un devoir de transparence sur ce sujet :

* Devoir de conseil du titulaire au titre de ses travaux,
* Devoir de communication du Ministère au titre des orientations internes pouvant impacter les travaux du titulaire.

# Documents applicables

## Documents de référence

Le PAS s’appuie sur un ensemble de documents de référence listés ci-dessous.

[A compléter]

* CCTP du Marché
* Référentiel Général de Sécurité de l’ANSSI (RGS) v2.0
* Norme ISO/IEC 27001:2013
* Politique de sécurité des systèmes d’information pour les Ministères chargés des affaires sociales (PSSI-MCAS)
* Charte relative à la protection de l’information et à la sécurité numérique des Ministères chargés des affaires sociales
* PSSI du titulaire (Le titulaire devra fournir la PSSI ou un document explicitant sa politique)
* ……………

## Procédures d’évolution du PAS

Le présent document doit faire l’objet d’une revue conjointe Ministère / Titulaire à minima une fois par an.

En cas de besoin d’évolution, le responsable du Titulaire (ou son représentant) et le RSSI (ou son représentant) échangeront afin de partager le besoin d’évolution. Ces évolutions pourront faire l’objet d’ateliers dédiés afin d’aboutir à l’évolution du document.

Dans le cas où la politique de sécurité du Ministère évoluerait et nécessiterait de revoir les procédures sécurité, ces travaux d’études et d’évolutions seraient à considérer comme un chantier à part entière.

Le document sera validé par le RSSI et présenté à l’ensemble des acteurs. La date de validation vaut date d’application.

## Applicabilité du PAS

Le Plan d’Assurance Sécurité est applicable à l’ensemble des acteurs du projet.

Un acteur du projet identifiant un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement au Responsable Sécurité du Titulaire, qui en avertira le RSSI et son équipe.

En cas de besoin, le Titulaire et le RSSI peuvent convenir d’une dérogation temporaire au PAS, spécifiant la forme de la demande, la liste de diffusion, les responsabilités des acteurs, et le planning.

# Cadre général de la prestation

## Description fonctionnelle de la prestation

Le présent marché a pour objet des prestations

## Lieux d’exécution

|  |  |
| --- | --- |
| ? | Donner la localisation précise de la prestation du titulaire |

[A compléter]

|  |  |
| --- | --- |
| ? | Présenter les sites et bâtiments utilisés dans le cadre de la prestation |

[A compléter]

|  |  |
| --- | --- |
| ? | Présenter les locaux utilisés dans le cadre de la prestation et indiquer leur catégorie (locaux techniques, bureaux, salle d’archive, etc.) |

[A compléter]

## Description de l’architecture

|  |  |
| --- | --- |
| ? | Fournir un schéma de l’architecture  Décrire l’architecture générale et les réseaux d’hébergement mis en œuvre pour assurer la prestation  Présenter les différents composants d’infrastructure utilisés (routeurs, commutateurs, firewalls, etc.)  Décrire les interconnexions avec les réseaux externes |

[A compléter]

## Ressources matérielles

|  |  |
| --- | --- |
| ? | Lister les ressources matérielles utilisées dans le cadre de la prestation : postes de travail, serveurs nécessaires au fonctionnement des postes de travail, serveurs applicatifs, composants d’infrastructure, …  Pour chaque ressource, préciser le fournisseur (titulaire, Ministère, sous-traitant) et décrire les fonctions assurées  Préciser la localisation réseau des différentes ressources  Préciser si les serveurs sont mutualisés avec d’autres clients ou activités. S’ils sont mutualisés, décrire les mesures de permettant d’assurer l’intégrité et la confidentialité des données relatives à la prestation et au Ministère |

[A compléter]

## Ressources logicielles

|  |  |
| --- | --- |
| ? | Lister les ressources logicielles utilisées dans le cadre de la prestation sur les différentes ressources matérielles  Préciser les éléments mis à disposition par le titulaire, par le Ministère, par un sous-traitant  Décrire les fonctions assurées par les différentes ressources |

[A compléter]

## Accès distants

|  |  |
| --- | --- |
| ? | Préciser si les accès distants sont autorisés.  Indiquer l’utilisation faite de ces accès distants et décrire les moyens mis en œuvre |

## Exigences de sécurité et mesures de protection

Dans le cadre de la sécurisation de son système d’information, **des Ministères Sociaux** ont mis en place une politique de sécurité des systèmes d’information.

Afin d’assurer la continuité des règles de sécurité applicables aux **Ministères Sociaux** certaines mesures doivent être couvertes par le titulaire. Si des mesures de la PSSI ne peuvent être mises en œuvre, pour quelques raisons que ce soit, il est nécessaire que ces éléments fassent l’objet d’un écrit, validés par le RSSI.

Pour l’ensemble des exigences de sécurité, il est attendu du titulaire que les réponses apportées soient précises complètes et vérifiables.

A cette fin, le titulaire formalise et documente chaque réponse et peut si nécessaire renvoyer vers des documents annexés à ce plan d’assurance sécurité.



# Cadre juridique

## Respect des contraintes sur les données à caractère personnel

**Exigence**

|  |
| --- |
| Si des données à caractère personnel sont stockées ou traitées dans le cadre de la prestation, le Titulaire doit justifier qu'il respecte toutes les exigences du Règlement Général sur la Protection des Données à caractère personnel (RGPD). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Résultats formalisés de l’étude RGPD |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Localisation géographique des services et des données

**Exigence**

|  |
| --- |
| Le Titulaire s’engage, sur le périmètre de la prestation, à spécifier préalablement et précisément les lieux géographiques dans lesquels sont localisés :  • Les données informatiques liées à la prestation  • Les services objets de la prestation  • Les personnes participant à la réalisation de la prestation  De même, le Titulaire précise si ses infrastructures (techniques ou organisationnelles) sont gérées par une entité juridique appartenant à un pays disposant de lois autorisant l’État à accéder aux données (ex. : « PatriotAct » aux Etats-Unis).  Le Titulaire s'engage à ne pas déplacer les données du Ministère sur un autre environnement que ceux définis dans la prestation, sans avoir préalablement reçu une autorisation formelle du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Indiquer notamment :  - La liste des lieux géographique d’hébergement des données (et des sites de backup)  - Les principes de remontée d’informations au Ministère en cas de modification en cours de contrat de localisation des lieux d’hébergement des données ou des services  - Pour le Titulaire et ses sous-traitants (tiers éditeur, tiers hébergeur, tiers exploitant, etc.) :  - Numéros de SIRET des établissements concernés  - Procédure de remontée d'informations vers le Ministère en cas de modification des lieux d'hébergement. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Certifications du Titulaire

**Exigence**

|  |
| --- |
| Si le Titulaire déclare qu’il dispose d’une certification applicable sur le périmètre de la prestation, il s’engage à fournir le justificatif de certification au Ministère. Le titulaire devra expliciter si les certifications sont applicables dans le cadre du contrat. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Préciser les certifications détenues et incluses dans le périmètre de la prestation ainsi que :  - La date du prochain contrôle de certification - Le périmètre défini dans le rapport de certification Indiquer si les rapports de certifications peuvent être communiqués au Ministère  - Certifications - Périmètres certifiés - Rapports de certification |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Répercussion des clauses sur les sous-traitants

**Exigence**

|  |
| --- |
| Le Titulaire s’engage, pour l’ensemble des informations manipulées et services mis en œuvre dans le cadre de la prestation, à spécifier précisément au Ministère les opérateurs (sociétés et fournisseurs) amenés à intervenir en cotraitance et sous-traitance.   Le Titulaire doit répercuter les clauses du présent PAS dans ses contrats de sous-traitance et de cotraitance et s’assurer de leur mise en œuvre effective.  Le Titulaire s'engage à respecter cette exigence dans le cas où un contrat de sous-traitance viendrait à être signé ultérieurement à la signature du contrat avec le Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Indiquer la liste des sous-traitants amenés à intervenir sur la prestation. Décrire comment les clauses du présent PAS sont appliquées et contrôlées auprès des sous-traitants du Titulaire.  - Liste et raison sociale des sous-traitants intervenant dans le cadre de la prestation - Dispositifs contractuels et opérationnels de répercussion des clauses du présent PAS auprès des sous-traitants (contrat, PAS, convention, etc.) - Principes de remontée d'informations vers le Ministère en cas de modification, en cours de contrat, de la liste des sous-traitants |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Organisation de la sécurité

## Responsabilités et rôles sécurité

**Exigence**

|  |
| --- |
| Le Titulaire doit désigner parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment : • L'interlocuteur privilégié du Ministère pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d’investigations initiées par le Ministère ou le Titulaire suite à des incidents de sécurité opérationnelle • Chargé du maintien et de la mise en application du PAS  Ce correspondant doit être joignable aux horaires convenus dans le cadre contractuel. Tout remplacement de ce correspondant doit être notifié au Ministère préalablement à son entrée en vigueur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Préciser la fonction de la personne responsable de la mise en œuvre et du respect du PAS (le nom et les coordonnées seront fournis dans l’annuaire de la prestation, ses rôles et missions seront détaillés dans le PAS ou document équivalent). Un engagement de devoir d’alerte en cas de changement de responsable est également attendu.  - Documents présentant le rôle, les responsabilités et les coordonnées du Responsable de la Sécurité de la Prestation (annuaire, PAS, support de sensibilisation). |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Existence d'une politique de sécurité

**Exigence**

|  |
| --- |
| Le Titulaire doit disposer d'une politique de sécurité ou a minima être conforme à la PSSI-MCAS |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Politique de sécurité. Le titulaire fera un comparatif des PSSI et indiquera les écarts avec la politique du Ministère. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Pilotage de la SSI

**Exigence**

|  |
| --- |
| Le Titulaire doit aborder les aspects sécurité dans le cadre de la gouvernance de la prestation. Il décrit, au PAS de la prestation ou tout document équivalent, les points suivants : • Les instances de pilotage de la prestation dans lesquelles la sécurité pourra être abordée • La fréquence à laquelle la sécurité sera abordée (au minimum trimestrielle)  • Les acteurs sécurité du Titulaire et du Ministère y participant  Le PAS, ou document équivalent, doit être validé par le Ministère au démarrage de la prestation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Le PAS, ou document équivalent, doit être validé par le Ministère au démarrage de la prestation.  - PAS de la prestation, ou document équivalent validé - Validation de la gouvernance sécurité par le Ministère (mail, compte-rendu, document version validée) |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Détection, alerte et traitement des incidents de sécurité

**Exigence**

|  |
| --- |
| Le Titulaire doit disposer, sur le périmètre de la prestation, d’un processus formalisé et opérationnel de gestion des incidents de sécurité. Celui-ci devra tenir compte des phases suivantes :  • détection,  • analyse,  • traitement, • alerte du Ministère Le Titulaire doit permettre au Ministère de participer au traitement de l’incident le cas échéant.  Des réunions périodiques d’analyse post-incident devront être planifiées avec le Ministère pour le traitement des causes profondes.  Le processus de gestion des incidents de sécurité doit être revu et approuvé par le Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| L'incident de sécurité est protéiforme, il peut être défini à partir de : - la typologie de l'évènement qui s'est produit,  - l'objectif de sécurité recherché, - la conformité d'un environnement dans un contexte donné.  Nous définirons un incident de sécurité SI par : un évènement potentiel ou avéré, indésirable ou inattendu, impactant la sécurité de l'information. L'impact sur la sécurité de l'information peut être évalué par rapport aux critères : Confidentialité, Intégrité, Preuve ou Disponibilité.  - Le processus de gestion des incidents de sécurité. Il doit décrire : o Intervenants, rôles, responsabilités et coordonnées o Mode opératoire de qualification, alerte, traitement et clôture des incidents de sécurité o Matrice de qualification des incidents de sécurité o Validation par le Ministère (bénéficiaire de la prestation) du processus de gestion des incidents de sécurité (mail, compte-rendu, document version validée) |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Gestion de crise sécurité

**Exigence**

|  |
| --- |
| Sur le périmètre SI de la prestation sous sa responsabilité, le Titulaire doit disposer d’un plan de gestion de crise formalisé et opérationnel tenant compte des aspects SSI.   Ce plan doit préciser au minimum : • Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ; • La composition de la cellule de crise : fonctions et responsabilités des membres (Ministère et Titulaire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ; • Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).  Le plan de gestion de crise doit être revu et approuvé par le RSSI du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| - Le plan de gestion de crise. Il doit décrire : - Intervenants, rôles, responsabilités et coordonnées - Mode opératoire de qualification, alerte, traitement et clôture d'une crise - Matrice de qualification d'une crise - Moyens utilisés en cas de crise (salle de crise (adresse postale, numéro de salle), moyens de télécommunication, annuaire) - Validation par le Ministère (bénéficiaire de la prestation) du plan de gestion de gestion de crise (mail, compte-rendu, document version validée) - Compte-rendu d'exercice de crise |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Base de connaissances

**Exigence**

|  |
| --- |
| Le titulaire doit capitaliser les procédures de résolution des incidents et problèmes de sécurité dans une base de connaissances dédiée. Il doit être en mesure de la fournir au Ministère sur demande. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Rapport de gestion des incidents de l'année passée, voire des années précédentes. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Engagement Individuel de Confidentialité (EIC)

**Exigence**

|  |
| --- |
| Le Ministère se réserve le droit de faire signer un engagement de confidentialité directement par le salarié et intervenant du Titulaire ou toute personne intervenant pour son compte. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Préciser qu’un engagement individuel de confidentialité sera signé par chaque collaborateur intervenant dans le cadre de la prestation. Un exemplaire devra être conservé par chacune des parties.  - Engagements Individuels de confidentialité signés - Document opérationnel de suivi des signatures |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Sensibilisation des intervenants

**Exigence**

|  |
| --- |
| Sur la base des informations transmises par le Ministère, le Titulaire s’engage à ce que chacun des intervenants sous sa responsabilité dans le périmètre de la Prestation respecte les règles de protection du Système d’Information du Ministère.   En complément, le Titulaire veille à ce que ses intervenants respectent les dispositions concernant la sécurité telles que décrites au Contrat et au présent PAS. Notamment : • L'organisation sécurité de la prestation • Le respect de la confidentialité tel que défini au contrat • Le signalement des incidents de sécurité ou des suspicions d’incidents de sécurité  Le Titulaire veille également à sensibiliser les populations sensibles selon leurs rôles et responsabilités en sécurité. Les administrateurs intervenant dans le cadre de la prestation devront notamment être sensibilisés aux thématiques suivantes :   * Les principales sources de risques externes * Phishing avancé * Notions de cryptographie * Sécurité réseau * Gestion des correctifs * Gestion des secrets * Mots de passe et comptes privilégiés * Gestion des logs   Cette sensibilisation doit être réalisée avant la prise de poste du personnel du Titulaire sur le périmètre de la Prestation, puis annuellement ou en cas d'évolution des règles de protection du Système d’Information du Ministère. Le Ministère pourra planifier et organiser avec le Titulaire des sessions de sensibilisation aux enjeux métiers. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Le Titulaire organise à sa charge la sensibilisation appropriée pour garantir le respect de ces mesures  Les règles de protection du Système d’Information du Ministère seront fournies au démarrage de la Prestation par le Ministère, notamment sous forme de documentation.  - Procédure de sensibilisation des intervenants du Titulaire (et sous-traitants) de la prestation (nom et fonction des personnes en charge de la sensibilisation, formation orale, fréquence des formations (au démarrage de la prestation et rappel annuel), émargement...) - Document support de la sensibilisation - Document opérationnel de suivi des signatures - Attestations individuelles de suivi de formation ou feuilles d'émargement. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Sensibilisation du personnel à la sécurité

**Exigence**

|  |
| --- |
| Le Titulaire doit organiser régulièrement des sessions de sensibilisation à la sécurité de l’information pour son personnel. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Plan de sensibilisation, précisant :   * Le calendrier des sessions de sensibilisation * Le contenu * Les moyens * La cible en termes de participants |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Audits et contrôles de sécurité

## Autocontrôle de sécurité

**Exigence**

|  |
| --- |
| Le Titulaire doit effectuer des autocontrôles de conformité aux exigences du présent PAS pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.  Il doit fournir et présenter au Ministère annuellement le tableau de bord des indicateurs sécurité formalisant le résultat de ces autocontrôles.   Le plan de contrôle présenté par le titulaire sera validé par le RSSI du Ministère; |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Les modalités de restitution des autocontrôles de conformité sont à définir avec le Ministère avant le démarrage de la prestation.  - Tableau de bord sécurité d'autocontrôle trimestriel complété ou résultats de l'autocontrôle |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Contrôles de sécurité

**Exigence**

|  |
| --- |
| Le Titulaire s'engage à autoriser le Ministère à réaliser des audits ou des contrôles de sécurité (« scan de vulnérabilité » ou « test d'intrusion informatique » par exemple), sans limite de nombre. Le Ministère prendra en considération l'impact de ces audits pour le Titulaire.  Sont entendus notamment que :  • Le Titulaire s'engage à collaborer de bonne foi avec le Ministère • Le rapport sera partagé avec le titulaire. • Le plan de remédiation sera construit avec le titulaire. • Le plan de remédiation précisera les acteurs et le calendrier de chaque action identifiée. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Le Titulaire spécifiera ici son accord ainsi que les modalités d'exécution et le délai de prévenance s'ils ne sont pas précisés au contrat.  À constater lors des contrôles : - Participation aux contrôles - Fourniture de preuves relatives aux exigences dans les délais fixés par les contrôleurs |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Contrôle des connexions distantes

**Exigence**

|  |
| --- |
| Le Titulaire doit mener à fréquence annuelle une analyse de vulnérabilités et un test d’intrusion pour chaque connexion distante utilisée dans le cadre de la Prestation (interconnexion avec les infogérants, connexion distante en astreinte). La réalisation des tests sera faite par un tiers.  Le Titulaire communiquera au Ministère la synthèse des résultats des tests notamment, la bonne réalisation des tests et la prise en compte d'un plan de remédiation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| La synthèse des derniers rapports de test d'intrusion ou de rapport de vulnérabilité. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Test de conformité des logiciels

**Exigence**

|  |
| --- |
| Le Titulaire effectuera des tests de conformité des postes et serveurs (ex : par le biais de routine), ainsi que les procédures et réactions liées aux remédiations  Le Titulaire décrira : \* La politique de conformité \* Les référentiels associés \* Le processus et la solution associée. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Les synthèses des rapports des derniers tests. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Sécurité des outils et services

**Exigence**

|  |
| --- |
| Le Titulaire démontre que les outils (outils mis en place par le titulaire pour aider dans le cadre de la prestation : Outil collaboratif, outil de ticketing, …) et services mis à disposition du Ministère ne sont pas sujets aux 10 principales vulnérabilités de l'OWASP. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Le Titulaire décrit ici les dispositifs mis en place pour assurer la détection des vulnérabilités de l'OWASP (types scan, audit et tests d’intrusion).  - Rapport des contrôles effectués au minimum une fois par an. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Correction des écarts identifiés

**Exigence**

|  |
| --- |
| En cas d’écarts constatés, avec les exigences de sécurité contractuelles, ou en cas de manquement à la sécurité, suite à un audit ou un contrôle, un plan de remédiation devra être formalisé par le Titulaire au plus tard 15 jours après la livraison du rapport. Le Titulaire devra ensuite régulariser ces écarts ou manquements par l'application du plan de remédiation dans un délai convenu en commun accord par les deux parties. En cas d’écarts constatés, avec les exigences de sécurité contractuelles, ou en cas de manquement à la sécurité, suite à un audit ou un contrôle, un plan de remédiation devra être formalisé par le Titulaire au plus tard 15 jours après la livraison du rapport. Le Titulaire devra ensuite régulariser ces écarts ou manquements par l'application du plan de remédiation dans un délai convenu en commun accord par les deux parties. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Les retards pourront donner lieu à des pénalités financières. Par ailleurs, des écarts trop importants peuvent être une cause de rupture de contrat.  - Plan d'actions de mise en conformité des écarts constatés lors des audits - Fourniture du plan d'actions dans les 15 jours suivant la constatation des écarts (date de remise du plan d'actions (mail, etc.)) |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Sécurité des environnements

## Protection contre les programmes malveillants

**Exigence**

|  |
| --- |
| Le Titulaire s’engage, dans le cadre de la prestation, à installer, sur les équipements qui le supportent (postes de travail et serveurs notamment), des systèmes de protection contre les codes malveillants, ainsi qu’à : • Les mettre à jour régulièrement,  • Ne pas les désactiver même à des fins de résolution d’incident. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| - Décrire les solutions en place sur les équipements de la prestation  - Décrire les politiques de gestion de ces solutions (fréquences de mise à jour des bases antivirales, fréquences de scans des ressources, etc.) - Formaliser l'engagement sur la non désactivation des dispositifs de protection en cas d’incident  - Description de la solution antivirus utilisée sur les équipements - Inventaire des équipements affectés à la prestation (postes de travail, serveurs, etc.) - Captures d’écran de la solution antivirus utilisée sur un échantillon d'équipements - Version de la dernière base de signature installée - Version du moteur antivirus et de l'agent antiviral - Captures d'écran de la console de gestion antivirale (nombre d'agents déployés sur les équipements, statut actif/inactif) |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Suivi de la protection contre les programmes malveillants

**Exigence**

|  |
| --- |
| Un suivi périodique (au minimum hebdomadaire) de l’état de mise à jour des systèmes de protection des postes de travail et serveurs du Titulaire contre les programmes malveillants (version, signatures antivirales) doit être effectué et formalisé. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire la procédure de suivi hebdomadaire du bon déploiement des mises à jour antivirales (récupération des signatures antivirales, déploiement, récupération des logs de déploiement des signatures, plan d’actions correctif en cas d’échec, etc.).  La procédure de suivi des antivirus précisant notamment : - Les principes et fréquences de mises à jour des anti-virus. - Les principes et fréquences des contrôles de l'application de cette procédure. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Correctifs de sécurité

**Exigence**

|  |
| --- |
| Le Titulaire s’engage, dans le cadre de la prestation, à maintenir à jour tous les composants logiciels et techniques qui concourent à la délivrance de l’objet de la prestation, dont : • Tous les logiciels et systèmes d’exploitation installés sur les équipements d’infrastructure ou réseau ; • Tous les logiciels et systèmes d’exploitation périphériques ; • Tous les logiciels de sécurité. Il s’engage notamment à réaliser une veille technique et à appliquer les correctifs de sécurité adéquats dans des délais adaptés à la prestation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire le système de déploiement et de surveillance des correctifs de sécurité sur les composants logiciels et techniques de la prestation (postes de travail, serveurs, équipements réseaux, logiciels, firmwares, librairies, etc.). En précisant pour chaque type de ressource : les systèmes d’exploitation, éditeurs, fréquences de déploiement, etc.  - Description du dispositif permettant le déploiement et la surveillance des correctifs de sécurité (Unix/Windows) sur les équipements (collecte, qualification, déploiement des mises à jour des correctifs de sécurité, périodicité des mises à jour, processus de validation d'un correctif, tests de non régression). - Inventaire des équipements affectés à la prestation (postes de travail, serveurs, etc.) - Référentiel des correctifs applicables et plan de déploiement. - Journal des installations des correctifs de sécurité sur un échantillon d'équipements. - Capture d’écran de la configuration du système de déploiement des correctifs de sécurité. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Suivi de l'application des correctifs de sécurité

**Exigence**

|  |
| --- |
| Un suivi périodique (mensuel) de l’état de mise à jour des correctifs de sécurité des composants logiciels et techniques du Titulaire doit être effectué et formalisé. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire la procédure de suivi hebdomadaire du bon déploiement des correctifs de sécurité (récupération des logs de déploiement, plan d’action correctif en cas d’échec, etc.).  - Politique(s) de déploiement des correctifs de sécurité. - Procédure de suivi de l’état des mises à jour des correctifs de sécurité des équipements (niveau de mise à jour de l'ensemble du parc informatique, personne en charge des contrôles, journalisation des contrôles, périodicité). - Suivi des mises à jour des correctifs de sécurité (compte rendu de suivi de déploiement mensuel des mises à jour). - Traces de suivi des mises à jour des correctifs de sécurité sur un échantillon d'équipements de la prestation. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Sécurité des données

## Gestion des données

**Exigence**

|  |
| --- |
| L’accès, le stockage, le marquage, l’échange et la destruction des documents et données doivent être sécurisés. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Document formalisé concernant la gestion des données et document lors des phases suivantes : - Echange des données - Accès aux données. - Stockage des données  Le document détaillera les principes de : - Marquage des données et documents. - Destruction des données. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Marquage des ressources techniques

**Exigence**

|  |
| --- |
| Le Ministère attend du Titulaire qu'il indique les règles de marquage qu'il applique sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Document précisant les règles de marquage des ressources nécessaires à la réalisation des prestations pour le Ministère. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Cloisonnement des données du Ministère

**Exigence**

|  |
| --- |
| Le Titulaire s’engage, dans le cadre de la prestation, à mettre en œuvre les moyens techniques et organisationnels pour couvrir les besoins de sécurité des données du Ministère, et notamment assurer qu’elles ne sont en aucune façon accessibles ou visibles par : • Les autres clients du Titulaire • Les intervenants du Titulaire qui n'ont pas le besoin d'en connaître.  Si la prestation prévoit l'hébergement d'environnements de production du Ministère, le Titulaire s’engage à mettre en œuvre et à maintenir un cloisonnement vis à vis des autres environnements (développement, recette, bureautique... par exemple). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire : - les moyens de cloisonnement prévus pour la protection des données du Ministère. - les engagements en termes de non-utilisation des données en dehors des environnements prévus dans le contrat.  Cette exigence couvre les données propriété du Ministère et également celles :  - hébergées sur des serveurs de fichiers et de messagerie du Titulaire - produites pour le Ministère (livrables)  - Schéma d’architecture - Configuration des VLAN  - GPO, ACL, etc. - DAT |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Sauvegarde de la base de données contenant les mots de passe

**Exigence**

|  |
| --- |
| Le Titulaire garantit la sauvegarde du gestionnaire de secrets des différentes ressources. Il effectuera des tests de restauration mensuels de cette base, dont les résultats devront être communiqués au Ministère.  Le Titulaire décrira la solution et le processus de réplication qu’il envisage. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Procédure formalisée précisant les principes de sauvegarde des identifiants et authentifiants des administrateurs.  Derniers rapports de contrôle d'application de cette procédure |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Sécurité des accès logiques

## Identifiants du Titulaire

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à définir et appliquer une politique de gestion des identifiants.  Il est attendu du Titulaire : • Que sa politique privilégie l'utilisation d’identifiants individualisés (rattachés à une personne unique) ; • Qu’il puisse expliciter comment il est en mesure de relier à tout instant l'usage d'un compte non individualisé avec l'identité d'une personne. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire : - Les règles de gestion des identifiants - Les règles de gestion des identifiants et des comptes génériques. Le cadre d’utilisation de ces comptes (finalités, cas d’usage, etc.)  - Politique de gestion des accès logiques - Capture d'écran d'un échantillon de comptes utilisés pour la prestation, sur chaque type de ressource. Tous les types de comptes utilisés doivent apparaître (comptes à privilèges, sans privilèges, compte nominatif et générique, etc.) - Liste des comptes génériques et leur contexte d'utilisation (expression du besoin) - Impression d’écran montrant que les comptes « invité » et les comptes créés par défaut lors de l’installation des serveurs intervenant dans le cadre de la prestation, sont bien désactivés ou renommés - Politique de gestion de revue des comptes prenant en charge la création/modification/suppression des droits d'accès |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Identifiants du Ministère

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire doit mettre à disposition un système de gestion individualisée des identifiants du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Pour répondre à cette exigence, le Titulaire privilégiera les solutions de type synchrone (Fédération d’Identité) exploitant les informations (identifiants / jetons / privilèges) issus de l’annuaire du Ministère.  Dans le cas d’une solution asynchrone (non fédérée) le Titulaire explicite comment sont opérées les identités : création / modification / suppression et qui est le garant de ce processus.  - Cahier des Charges (CDC) ou autre document formalisant le besoin en termes d’identification ; - Capture d'écran prouvant la mise en œuvre des besoins en termes de gestion des identifiants du Ministère sur les ressources de la prestation ; - Procédure de la prestation de gestion des identifiants du Ministère (création/suppression/modification). |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Authentification du Titulaire en administration

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à mettre en place une politique de gestion des authentifiants, pour ses accès en administration. Cela se traduit notamment par :  • L’utilisation de mots de passe de longueur minimale conforme à la PSSI/norme de l’ANSSI • Une politique de renouvellement, conforme à la PSSI/norme de l’ANSSI • L’utilisation de mots de passe contenant les quatre familles de caractères (lettres minuscules, lettres majuscules, chiffres, caractères spéciaux) conforme à la PSSI/norme de l’ANSSI • L’utilisation de systèmes d’authentification à plusieurs facteurs pour les accès distants.  Les sessions (système ou applicatives) doivent être protégées par des mécanismes de verrouillage automatiques en cas d'inactivité prolongée (au maximum après 10 minutes). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire la politique de mot de passe appliquée sur le périmètre de la prestation notamment dans le cadre des accès d’administration. Préciser les éventuelles procédures d’accès distant.  - Politique de mots de passe administrateurs fonctionnels et techniques du Titulaire utilisée dans le cadre de la prestation   Capture d'écran des politiques de mot de passe implémentée (ex. : GPO sous Windows) sur les serveurs, équipements réseau et postes de travail (comptes administrateurs) indiquant : 1) La robustesse du mot de passe en termes de longueur et de complexité suivant les quatre familles de caractères disponibles ; 2) La durée de vie du mot de passe.  - Procédure d'accès distant des administrateurs Titulaires à l'infrastructure hébergeant la prestation - Capture d’écran du paramétrage des mécanismes de verrouillage automatique en cas d’inactivité prolongée sur les ressources de la Prestation. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Authentification du Titulaire sur les actions d'administration

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à mettre en place l'utilisation de systèmes d’authentification à plusieurs facteurs pour les actions d'administrations techniques et fonctionnelles, locales ou distantes. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Documents précisant les règles liées à l'identification et authentification des administrateurs techniques et fonctionnels |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Authentification des utilisateurs du Ministère, des prestataires et des intervenants du Titulaire

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à mettre en place une politique de gestion des authentifiants conforme aux besoins de sécurité du Ministère. Cela se traduit au minimum par :  • La possibilité d’utiliser des mots de passe de plus de 8 caractères conforme à la PSSI/norme de l’ANSSI • L’utilisation de mots de passe contenant au moins trois parmi les quatre familles de caractères (lettres minuscules, lettres majuscules, chiffres, caractères spéciaux) conforme à la PSSI/norme de l’ANSSI • Verrouillage ou temporisation en cas de plusieurs tentatives infructueuses. ( supérieure à 1 minute après 5 tentatives échouées, et maximum de 25 tentatives par 24 heures; et/ou – un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives) conforme à la PSSI/norme de l’ANSSI \* un blocage du compte après un nombre d’authentifications échouées consécutives au plus égal à 10. • Une politique de renouvellement, au maximum tous les 90 jours.  Si le Ministère met à disposition un système d’authentification à plusieurs facteurs, le Titulaire s'engage à les utiliser conformément aux procédures fournies par le Ministère.  Les sessions (systèmes ou applicatives) doivent être protégées par des mécanismes de verrouillage automatique en cas d'inactivité prolongée (au maximum après 15 minutes). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire les authentifiants du Ministère que le Titulaire compte opérer et la politique de mot de passe associée.  - Politique de mots de passe utilisateurs - Capture d'écran des politiques de mot de passe implémentées (ex GPO sous Windows) sur les postes de travail (administrateurs) indiquant : 1) Robustesse du mot de passe en termes de longueur et de complexité suivant trois parmi les quatre familles de caractères disponibles  2) La durée de vie du mot de passe - Capture d’écran du paramétrage des mécanismes de verrouillage automatique en cas d’inactivité prolongée sur les ressources de la Prestation. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Authentification des utilisateurs du Ministère et des intervenants du Titulaire

**Exigence**

|  |
| --- |
| le Titulaire s’engage à mettre en place l'utilisation de systèmes d’authentification à plusieurs facteurs pour l'ensembles des utilisateurs accédant aux données ou à l'application. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Documents précisant les règles liées à l'identification et authentification des utilisateurs |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Gestion des privilèges

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à mettre en place une politique de gestion des privilèges conforme aux bonnes pratiques de sécurité, se traduisant notamment par l'attribution des habilitations selon le principe de moindre privilège et du besoin d'en connaître. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire les différentes typologies de profils existantes et les droits associés ainsi que les processus mis en place pour s’assurer que ces privilèges sont bien respectés. Préciser notamment les droits accordés aux utilisateurs sur leur poste de travail et sur les serveurs (utilisateur standard, utilisateurs avec pouvoirs, admin local. Principe de moindre privilège : principe selon lequel chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches.  - Procédure de gestion des comptes à privilèges - Impression d’écran de la liste des comptes à privilèges de la prestation - Description des profils des comptes à privilèges utilisés dans le cadre de la prestation - Expression du besoin d’utilisation des comptes à privilèges. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Revue et suivi des comptes du domaine de responsabilités du Titulaire

**Exigence**

|  |
| --- |
| Une revue périodique\* des comptes d’accès aux ressources informatiques (serveurs, postes de travail, applications) du Titulaire utilisées dans le cadre de la prestation doit être effectuée et formalisée. \* Une revue « d’emploi » (au minimum trimestrielle), une revue de « besoin » (au minimum annuelle). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire les procédures de revue sur les ressources du SI du Titulaire (postes de travail, serveurs, équipements réseaux) : modes opératoires, périodicités, responsabilités, plan d’action en cas d’écart, etc.  La revue d’emploi consiste à vérifier que les comptes présents dans le système correspondent aux profils des intervenants (comptes d’accès, logiciels autorisés, etc.). Il s’agit également de vérifier que les comptes des collaborateurs ayant quitté la prestation sont bien désactivés sur le périmètre de la prestation. La revue de « besoin » consiste à vérifier que les droits attribués à chaque profil des intervenants correspondent aux besoins pour mener à bien leurs missions.   * Procédure opérationnelle de revue des comptes * Preuve (PV, mail, compte-rendu) de revue d'emploi et de besoin |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Traçabilité des accès logiques

**Exigence**

|  |
| --- |
| Durant l'exécution de la prestation, le Titulaire met en place, sur ses ressources, des traces qui assurent à tout instant l'imputabilité des actions réalisées. Ces traces contiennent notamment (en fonction de la typologie des ressources) :  • L'identifiant de l'accédant • Les connexions et déconnexions aux ressources  • Les accès fructueux et infructueux aux ressources • L'origine des connexions  • Les actions réalisées (modification, suppression...) • Les informations d'horodatage  et ce pendant une durée au minimum d’un an et en accord avec les exigences légales et réglementaires. Ces traces doivent pouvoir être fournies sur demande du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire le dispositif de traçabilité des accès aux ressources du SI Titulaire (contenu des logs, sauvegarde des logs, localisation des sauvegardes, durée de conservation, exploitation éventuelle des logs etc.)  Les ressources du SI Titulaire sont les serveurs et applications utilisés dans le cadre de la prestation. Les accédants sont les utilisateurs et les administrateurs du Titulaire.  Document précisant les moyens techniques et organisationnels assurant la traçabilité des accès aux ressources. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Suivi des mécanismes de traçabilité des accès logiques

**Exigence**

|  |
| --- |
| Le Titulaire doit s'assurer mensuellement du bon fonctionnement des dispositifs de traçabilité :  • Collecte effective des traces  • Sauvegarde effective de ces traces.  De plus, le Titulaire s'engage à ne pas désactiver les dispositifs de traçabilité mis en place. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| A titre d’exemple, le Titulaire pourra mettre en œuvre, pour répondre à cette exigence, un processus de suivi périodique du bon enregistrement des traces ou un dispositif d'alerte en cas de non-enregistrement et le type de plan d'action en cas d'échec.  - Procédure de suivi du bon enregistrement des traces sur les ressources système et applicatives - Compte-rendu ou autre preuve de suivi opérationnel du bon enregistrement des traces |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Détection des anomalies de gestion des accès

**Exigence**

|  |
| --- |
| Une procédure permettant de détecter, a posteriori, des anomalies dans la gestion des autorisations (badge ou carte non restitués, utilisation d'un badge perdu, faux badge, etc.) doit être formalisée et respectée. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Document formalisant les moyens techniques et procéduraux pour la gestion des accès logiques, notamment l'identification d'anomalies dans cette gestion des accès. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Sécurité réseau

## Politique de gestion des flux réseau

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à mettre en place une politique de gestion des flux réseau, afin de n’autoriser que les flux légitimes. Par défaut, tous les flux qui ne sont pas explicitement autorisés doivent être interdits. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire les règles de filtrage des équipements réseau  - Politique ou processus de gestion des flux réseau (ouverture, modification, fermeture, etc.) - Capture d’écran, au niveau des firewall, de la règle de filtrage : « tout ce qui n’est pas explicitement autorisé est interdit ». |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Cartographie des flux

**Exigence**

|  |
| --- |
| Sur le périmètre de la prestation, le Titulaire s’engage à : • Fournir une matrice exhaustive et à jour des flux mis en œuvre au démarrage de la Prestation, • Maintenir à jour cette matrice des flux et informer le Ministère de toute évolution, • Effectuer une revue semestrielle de cette matrice. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire le processus de gestion des matrices de flux (définition, maintien, revue).  - Processus de gestion des matrices de flux - Matrice des flux techniques avec cartouche des modifications (gestion des versions) - CR de la dernière revue de la matrice de flux - DAT |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Chiffrement des flux

**Exigence**

|  |
| --- |
| Le Titulaire s’engage, dans le cadre de la Prestation, à mettre en place et à maintenir les moyens techniques utiles au chiffrement de tous les flux qui le nécessitent, dont au minimum :  • Tous les flux d’authentification des utilisateurs et des administrateurs • Tous les flux relatifs à des accès distants • Tous les flux spécifiquement mentionnés au contrat |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire les moyens de chiffrement de flux prévus sur le périmètre de la Prestation.  - Matrice des flux techniques - Capture d'écran de la configuration des flux d'authentification, des flux relatifs aux accès distants et des flux spécifiques à la prestation (ex: https, VPN) - DAT |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Chiffrement des échanges inter-sites

**Exigence**

|  |
| --- |
| Le Titulaire doit chiffrer les échanges entre ses différents sites ou lieux de travail et le processus mis en place devra être soumis au préalable au Ministère pour accord. La fourniture des moyens nécessaires, les frais de mise en place et liés à l’utilisation de ces moyens de chiffrement seront à la charge du Titulaire. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Document précisant les moyens techniques permettant d'assurer les chiffrements des échanges inter-sites |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Prévention contre les attaques externes

**Exigence**

|  |
| --- |
| Le Titulaire mettra en œuvre des dispositifs afin de prévenir les attaques informatiques (intrusion, déni de service, brute force…) sur le SI utilisé dans le cadre de la prestation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire les moyens techniques et organisationnels mis en place afin de protéger le service objet de la prestation contre les intrusions (sondes IPS/IDS, firewall applicatif, etc.).  - DAT ou équivalent décrivant les dispositifs de protection  - Enregistrements d'accès non autorisés capturés par les sondes IPS/IDS et/ou firewall(s) - Capture d’écran, au niveau du firewall, de la règle de filtrage : « tout ce qui n’est pas explicitement autorisé est interdit » |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Traçabilité des accès réseau

**Exigence**

|  |
| --- |
| Les équipements réseau du Titulaire, dans le cadre de la prestation, doivent enregistrer et protéger les traces d’accès au réseau / service, dont au minimum :  • L'adresse IP de l’émetteur,  • L'adresse IP du destinataire,  • La date,  • L'heure,  et ce pendant 1 an ou en accord avec les exigences légales et réglementaires en vigueur. Ces traces doivent pouvoir être fournies sur demande du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire le dispositif d’enregistrement des traces des équipements réseau (fréquence d’enregistrement, détails des informations enregistrées, délai de rétention, etc.)  - Politique de gestion des traces spécifiant la durée de conservation et les méthodes de conservation de ces traces (lieu de stockage, duplication, accès, etc.)  - Capture d'écran indiquant l'activation du paramètre d'audit sur les équipements réseaux - Exemple de trace réseau d’une transaction sur le périmètre de la prestation |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Suivi des mécanismes de traçabilité des accès réseau

**Exigence**

|  |
| --- |
| Le Titulaire doit s'assurer mensuellement du bon fonctionnement des dispositifs de traçabilité :  • Collecte effective  • Sauvegarde effective des traces. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| A titre d’exemple, le Titulaire pourra mettre en œuvre pour répondre à cette exigence, un processus de suivi périodique du bon enregistrement des traces ou un dispositif d'alerte en cas de non-enregistrement et le type de plan d'action en cas d'échec.  - Procédure de suivi du bon enregistrement des traces sur les ressources réseau - Compte-rendu ou autre preuve de suivi opérationnel du bon enregistrement des traces |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Sécurité physique

## Contrôle des accès physiques aux locaux du Titulaire

**Exigence**

|  |
| --- |
| Les locaux du Titulaire, hébergeant les intervenants dans le cadre de la prestation, doivent être équipés d’un dispositif de contrôle d’accès individuel. Toute tentative d’accès à ces locaux doit faire l’objet d’une trace qui doit être conservée au minimum 2 mois. Le Titulaire restreint ces accès physiques aux stricts besoins opérationnels.   Une procédure de gestion des accès physiques aux locaux du Titulaire doit être formalisée. Celle-ci doit préciser au minimum les modalités de gestion des demandes et suppressions d’accès ainsi qu'une revue trimestrielle. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire le dispositif de contrôle d’accès physique individuel des bâtiments et plateaux où seront localisés les collaborateurs de la prestation (dispositif d’identification, sas d’accès, traçabilité)  - Procédure de gestion des accès physiques au bâtiment. - Documentation du dispositif de contrôle d’accès individuel aux bâtiments - Photos du dispositif de contrôle d’accès physique - Description de la solution/outil de GTB (Gestion technique de Bâtiment) - Extraction des traces d’accès aux locaux hébergeant les intervenants dans le cadre de la prestation |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Respect des normes de sécurité physiques et environnementales

**Exigence**

|  |
| --- |
| Le Titulaire doit détailler les mesures mises en œuvre afin de garantir la sécurité physique et environnementale des locaux hébergeant son personnel. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Plan de sécurisation du site et des salles d'hébergement concernant la prestation réalisée.  \* Gestion des accès physiques. \* Servitude et secours des servitudes (Energie et climatisation). \* Détection et protection incendie |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Contrôle des accès physiques aux ressources techniques du Titulaire

**Exigence**

|  |
| --- |
| Les locaux qui hébergent les ressources techniques du Titulaire doivent être équipés d’un dispositif de contrôle d’accès individuel. Toute tentative d’accès à ces locaux doit faire l’objet d’une trace qui doit être conservée au minimum 2 mois. Le Titulaire restreint ces accès physiques aux stricts besoins opérationnels.   Une procédure de gestion des accès physiques aux locaux techniques du Titulaire doit être formalisée. Celle-ci doit préciser au minimum les modalités de gestion des demandes et suppressions des accès ainsi qu'une revue trimestrielle. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire le dispositif de contrôle d’accès physique individuel des locaux techniques hébergeant les serveurs de données, d’infrastructure et de l’équipement réseau / télécoms (dispositif d’identification, sas d’accès, traçabilité).  - Procédure de gestion des accès physiques aux locaux techniques. - Documentation du dispositif de contrôle d’accès individuel aux locaux techniques - Photos du dispositif de contrôle d’accès physique mis en place au niveau du local technique. - Extraction des traces d’accès aux locaux hébergeant les ressources techniques du Titulaire |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Protection contre le vol

**Exigence**

|  |
| --- |
| Le Titulaire doit mettre en place des mécanismes de protection pour prévenir les vols de terminaux mobiles utilisés dans le cadre de la prestation et réduire leurs impacts. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Par terminaux mobiles sont entendus : postes de travail, ordinateurs portables, tablettes, téléphones. Le Titulaire s'engage notamment à mettre en place des câbles antivol sur les postes de travail de façon systématique.  - Description et photos des dispositifs de protection des postes de travail (câble antivol, etc.) - Description des dispositifs de réduction des impacts en cas de vol de terminaux mobiles (destruction des données à distance, chiffrement, géo localisation, etc.). |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Protection des plateaux mutualisés

**Exigence**

|  |
| --- |
| En cas de mutualisation de ses plateaux, le Titulaire devra démontrer les mesures mises en place pour protéger les espaces attribués pour la prestation effectuée pour le Ministère (accès au poste par badge, blocage session automatique après un certain temps d’inutilisation, câble de sécurité pour le matériel fourni par le Ministère, etc.). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Procédure formalisée et plan de sécurisation des locaux mutualisés. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Sécurité lors de la réversibilité

## Maintien de la sécurité durant la réversibilité ou transfert de la prestation

**Exigence**

|  |
| --- |
| En cas d'arrêt de la prestation (fin de contrat ou activation de la clause de réversibilité par exemple), pendant toute la durée de la phase de transfert associée, le Titulaire doit assurer le maintien du niveau de sécurité de la prestation décrit dans les documents contractuels.   Pour le respect de certaines exigences légales, les exigences du présent PAS liées à la conservation des traces sont toujours applicables après l’arrêt de la prestation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Procédure précisant : \* les principes de réversibilité \* Le périmètre \* Les moyens techniques et organisationnels |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Destruction des données en fin de prestation

**Exigence**

|  |
| --- |
| Le Titulaire doit disposer d’une procédure permettant la restitution et la destruction définitive des données du Ministère Cette procédure décrit notamment : • La destruction des données présentes sur tous les environnements (production, pré-production, qualification, développement…)  • La destruction des données présentes sur des supports de sauvegarde, même si ceux-ci sont mutualisés. Le Titulaire doit informer le Ministère sur le délai de destruction effective de ces données. Le Titulaire doit fournir un rapport de destruction qui mentionne au minimum :  • Le succès ou l’échec de l’opération • Les algorithmes ou la méthode utilisée pour la destruction   Cette exigence court jusqu’à la destruction effective des données (exemple : logs, données fiscales…). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Décrire la procédure de transfert et de destruction utilisée dans sur le périmètre de la prestation. Préciser la clause contractuelle liée à cette exigence s’il y a lieu.  *- Processus de restitution des données.*  - Procédure décrivant les mécanismes permettant la restitution et la destruction définitive des données - Description des moyens de destruction des données - PV de destruction des données (modèle ou document complété si une destruction a déjà eu lieu) |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Métiers

## Dispositif de validation des modifications

**Exigence**

|  |
| --- |
| Toute modification d'un environnement de production, effectuée par le personnel du Titulaire, devra avoir été préalablement validée par le Ministère (processus de gestion des changements, comité de validation, suivi des implémentations).  N.B : le SI de Production géré par le Titulaire est soit propriété du Ministère, soit déployé par le Titulaire. Dans un cas comme dans l'autre, toute évolution du SI de Production devra être intégrée dans les demandes courantes d’évolution du SI du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Procédure de validation avant modification. Exemple de validation de modification déjà réalisée. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Sécurité des mises en production

**Exigence**

|  |
| --- |
| Le Titulaire est garant de la fiabilisation des mises en production dont il a la responsabilité dans le cadre de la Prestation.  Le Ministère attend du Titulaire qu'il décrive les moyens prévus dans le cadre de la Prestation (recette, possibilité de retour arrière...). |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Procédure formalisée précisant les principes de vérification avant mise en production et les précautions prises en termes de retour arrière. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Règles de sécurité et d'exploitation

**Exigence**

|  |
| --- |
| L’installation, l’exploitation et l’administration des moyens mis en œuvre dans le cadre des Prestations devront être conformes aux bonnes pratiques et aux règles de sécurité et d’exploitation établies par le Ministère. Toute exception fera l'objet d'un accord préalable écrit des équipes du Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Procédures d'exploitation et d'administration intégrant les règles de sécurité. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Sources d'installations des logiciels

**Exigence**

|  |
| --- |
| Le Titulaire doit disposer des sources d’installation des logiciels utilisés dans le cadre de la Prestation, lorsque ces logiciels ne sont pas mis à disposition par le Ministère. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Liste des logiciels utilisés dans le cadre de la prestation. Liste des logiciels non mise à disposition par le Ministère. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Validité des licences

**Exigence**

|  |
| --- |
| Le Titulaire devra s'assurer de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou du Ministère dans le cadre de la Prestation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Liste des licences et dates de validité des licences |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Identification et traitement des vulnérabilités

**Exigence**

|  |
| --- |
| Le Titulaire doit mettre en place les dispositions afin d’identifier et traiter les vulnérabilités des produits fournis au Ministère.  Le titulaire doit mettre les mêmes dispositifs pour ses matériels/services utilisés pour couvrir la prestation. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Documents présentant les moyens techniques et organisationnels visant à identifier et traiter les vulnérabilités sur le périmètre de la prestation réalisée. Comptes rendu des dernières actions réalisées sur la gestion des vulnérabilités. |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

## Phase de réversibilité en fin de contrat

**Exigence**

|  |
| --- |
| Le Titulaire doit s’engager à assurer une phase de réversibilité en fin de contrat garantissant au Ministère le portage des services offerts. En particulier, le Titulaire doit s'engager à livrer la documentation nécessaire à la bonne réversibilité. |

**Commentaires et exemple de preuves attendues**

|  |
| --- |
| Cette documentation nécessaire à la bonne réversibilité comprend notamment le Dossier d'Architecture Technique (DAT).  Plan de réversibilité intégrant les principes de mise à jour. Dossier d'architecture technique |

**Réponse du titulaire**

|  |
| --- |
| A COMPLETER |

# Annexes

Le titulaire peut annexer à ce présent document, les documents complets et validés décrivant les mesures listées dans les précédents chapitres.

## Annexe 1 : Documents sécurité liés à la prestation

Les tableaux suivants listent les documents constitués et maintenus par le Titulaire durant toute la prestation.

## Suivi sécurité

| Catégorie | Documents |
| --- | --- |
| Annuaire et habilitations | * Annuaire des intervenants sur les aspects :   + Contractuel   + Technique   + Sécurité * Liste des personnes habilitées dans les locaux * Liste des comptes d’accès sur les postes de travail et serveurs, ainsi que les intervenants associés * Liste des intervenants disposant de droits d’administration |
| Inventaire | * Comptes rendus d’inventaire. |
| Engagements individuels de confidentialité signés | * Engagements de confidentialité, signés par tous les intervenants |
| Chartes d'utilisation des moyens de communication électronique signées | * Chartes d'utilisation des moyens de communication électronique, signées par tous les intervenants disposant d’un accès au SI du Ministère. |
| Suivi sessions de sensibilisation et des formations | * Pour chaque intervenant, liste des sessions de sensibilisations et des formations suivies * Comptes rendus d'actions sécurité (sensibilisation, formation) |
| Tableaux de bords sécurité | * Tableaux de bords sécurité |
| Revue des droits | * Synthèse trimestrielle de la revue périodique des comptes d’accès sur les ressources du Titulaire |
| Audit et contrôle | * Comptes rendus d’audit, de test d’intrusion et de contrôle interne (identification des vulnérabilités et du plan d’actions associé) * comptes rendus d’audit externe (identification des vulnérabilités et du plan d’actions associé) |
| Incidents de sécurité | * Comptes rendus d’incidents ou de problèmes qui émergent en cours de la prestation |
| Maintenance | * Comptes rendus d’opération de maintenance sur les produits de sécurité |
| [A compléter] | * [A compléter] |

## Organisation, processus et procédures sécurité

| Document | Contenu |
| --- | --- |
| Organigramme sécurité | * Organigramme sécurité |
| Politique de sécurité prestation (optionnel) | * Document de politique de sécurité associé à la prestation, regroupant notamment toutes les exigences de sécurité du Client |
| Politique d’habilitation | * Politique d’habilitation (accès physiques et logiques) |
| Politique de contrôle | * Politique de contrôle |
| Processus de gestion des vulnérabilités | * Processus, procédures et outils de gestion des vulnérabilités |
| Processus de gestion des incidents de sécurité | * Processus, procédures et outils de gestion des incidents de sécurité |
| Dossier d’architecture et sécurité du contrat | * Description des mesures et outils de sécurité utilisés pour assurer la sécurité des postes de travail et serveurs * Description du réseau d’hébergement et de l’interconnexion avec le SI du Ministère * Liste des flux autorisés et interdits * Description des mesures et outils de sécurité utilisés pour assurer la protection des informations * Description des moyens organisationnels et techniques assurant la traçabilité des accès physiques et logiques |
| Continuité de service | * Plan de sauvegarde détaillé * Plan de secours informatique * Plan de secours utilisateurs |
| Plan des locaux | * Plan des locaux, comprenant la localisation des locaux dédiés à la prestation, des locaux techniques, des contrôles d’accès physiques et des ressources matériels (postes de travail, serveurs, etc.) |
| PCA | * Processus et procédures de PCA |
| [A compléter] | * [A compléter] |

## Annexe 2 : Procédure XXXXX

## Annexe 3 : Politique XXXX