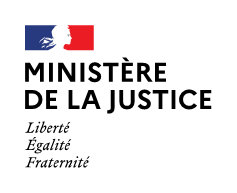
#### 



**Plan d’Assurance Sécurité – TITULAIRE – Contrat**

|  |  |  |
| --- | --- | --- |
| Version - Date | Emetteur | Statut/Suivi des modifications |
| Version 0.1  Novembre 2021 | B2SI | provisoire |
|  |  |  |
|  |  |  |
|  |  |  |

Table des matières

[1. Présentation du P.A.S. 4](#_Toc87973041)

[1.1. Objet 4](#_Toc87973042)

[1.2. Glossaire et définitions 4](#_Toc87973043)

[1.3. Documents de référence et associés 4](#_Toc87973044)

[1.3.1. Documents du MINISTERE DE LA JUSTICE : 4](#_Toc87973045)

[1.3.2. Documents du titulaire : 4](#_Toc87973046)

[2. Description de la prestation 4](#_Toc87973047)

[2.1. Le service rendu 4](#_Toc87973048)

[2.2. Description technique du système d’information du prestataire 4](#_Toc87973049)

[2.3. Périmètre d’application de la sécurité 4](#_Toc87973050)

[2.4. Gestion des évolutions 7](#_Toc87973051)

[3. Enjeux et objectifs de la SSI 7](#_Toc87973052)

[3.1. Enjeux en matière de SSI 7](#_Toc87973053)

[3.2. Objectifs en matière de SSI 7](#_Toc87973054)

[4. Organisation de la SSI 7](#_Toc87973055)

[4.1. Organisation de la cyber sécurité (Sécurité des Systèmes d’Information) 7](#_Toc87973056)

[4.1.1. Chaîne décisionnelle de cyberdéfense (SSI) 7](#_Toc87973057)

[5. Pilotage de la cyber sécurité 7](#_Toc87973058)

[5.1. Cadre de référence appliqué 7](#_Toc87973059)

[5.2. Principes fondateurs 7](#_Toc87973060)

[5.1.1. Assurer une amélioration continue 8](#_Toc87973061)

[5.1.2. Analyser et traiter les risques 8](#_Toc87973062)

[5.1.3. Sensibiliser et former 8](#_Toc87973063)

[5.1.4. Réaliser la veille sécurité et réglementaire 8](#_Toc87973064)

[5.1.5. Prévoir et gérer la réponse aux incidents de sécurité 9](#_Toc87973065)

[5.1.6. Piloter la sécurité sur les bases d’indicateurs factuels et d’objectifs chiffrés 9](#_Toc87973066)

[6. Responsabilités liées au PAS 9](#_Toc87973067)

[7. Validation et diffusion 9](#_Toc87973068)

[7.1. Procédure en cas de non-application et demande de dérogation 9](#_Toc87973069)

[8. Procédures d’évolution du PAS 9](#_Toc87973070)

[9. Mesures de sécurité appliquées 9](#_Toc87973071)

[9.1. Ressources humaines 10](#_Toc87973072)

[9.1.1. Avant l’embauche 10](#_Toc87973073)

[9.1.2. Pendant la durée du contrat 10](#_Toc87973074)

[9.1.3. Rupture, terme ou modification du contrat de travail 10](#_Toc87973075)

[9.2. Gestion des biens 10](#_Toc87973076)

[9.2.1. Cartographie des SI 10](#_Toc87973077)

[9.2.2. Qualification et protection de l’information 10](#_Toc87973078)

[9.3. Intégration de la SSI dans le cycle de vie des systèmes d'information 10](#_Toc87973079)

[9.3.1. Gestion des risques et homologation de sécurité 10](#_Toc87973080)

[9.3.2. Maintien en condition de sécurité des systèmes d’information 10](#_Toc87973081)

[9.3.3. Produits et services labellisés 10](#_Toc87973082)

[9.3.4. Gestion des prestataires 11](#_Toc87973083)

[9.4. Sécurité Physique 11](#_Toc87973084)

[9.5. Sécurité des réseaux 11](#_Toc87973085)

[9.5.1. Sécurité des réseaux nationaux (sécurisation des flux) 11](#_Toc87973086)

[9.5.2. Sécurité des réseaux locaux 11](#_Toc87973087)

[9.5.3. Accès spécifiques 11](#_Toc87973088)

[9.5.4. Sécurité des réseaux sans fil 11](#_Toc87973089)

[9.5.5. Sécurisation des mécanismes de commutation et de routage 12](#_Toc87973090)

[9.5.6. Cartographie réseau 12](#_Toc87973091)

[9.6. Architecture des SI 12](#_Toc87973092)

[9.6.1. Architecture des centres informatiques 12](#_Toc87973093)

[9.7. Exploitation des SI 12](#_Toc87973094)

[9.7.1. Protection des informations sensibles 12](#_Toc87973095)

[9.7.2. Sécurité des ressources informatiques 12](#_Toc87973096)

[9.7.3. Gestion des autorisations et contrôle d’accès logique aux ressources 12](#_Toc87973097)

[9.7.4. Exploitation sécurisée des ressources informatiques 12](#_Toc87973098)

[9.7.5. Défense des systèmes d’information 13](#_Toc87973099)

[9.7.6. Exploitation des centres informatiques 13](#_Toc87973100)

[9.8. Sécurité du poste de travail 13](#_Toc87973101)

[9.8.1. Sécurisation des postes de travail 13](#_Toc87973102)

[9.8.2. Sécurisation des imprimantes et copieurs multifonctions 13](#_Toc87973103)

[9.8.3. Sécurisation de la téléphonie 13](#_Toc87973104)

[9.8.4. Contrôles de conformité 13](#_Toc87973105)

[9.9. Sécurité du développement des systèmes 13](#_Toc87973106)

[9.10. Traitements des incidents 13](#_Toc87973107)

[9.10.1. Chaînes opérationnelles 13](#_Toc87973108)

[9.11. Continuité d'activité 13](#_Toc87973109)

[9.11.1. Gestion de la continuité d’activité des SI 13](#_Toc87973110)

[9.12. Conformité, audit, inspection, contrôle 13](#_Toc87973111)

[9.12.1. Conformité avec les exigences légales et règlementaires 14](#_Toc87973112)

[9.12.2. Conformité avec les politiques de sécurité 14](#_Toc87973113)

[9.12.3. Revue de la sécurité de l’information 14](#_Toc87973114)

[9.12.4. Contrôles 14](#_Toc87973115)

[10. Couverture des exigences de sécurité 14](#_Toc87973116)

# 1. Présentation du P.A.S.

## Objet

Présentation de la mission rendue :

Description du périmètre technique et contractuel :

## 1.2. Glossaire et définitions

## 1.3. Documents de référence et associés

### 1.3.1. Documents du MINISTERE DE LA JUSTICE :

### 1.3.2. Documents du titulaire :

# 2. Description de la prestation

## 2.1. Le service rendu

(Description de la prestation en conformité avec le CCTP)

## 2.2. Description technique du système d’information du prestataire

(Schéma d’architecture et spécifications techniques du SI utilisé pour réaliser la mission pour Le MINISTÈRE DE LA JUSTICE).

## 2.3. Périmètre d’application de la sécurité

(Sélectionner)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Numéro** | **Thème de l'objectif** | **Nom de l'objectif** | **Description** | **Retenu ?** |
| ***1*** | **Organisation de la sécurité des systèmes d’information** | Organisation de la sécurité des systèmes d’information | Organisation de la SSI. Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité. | **Oui** |
| ***2*** | **Ressources humaines** | Ressources humaines | Ressources humaines. Faire des personnes les maillons forts des SI de l’État. | **Oui** |
| ***3*** | **Gestion des biens** | Cartographie des SI | Cartographie des SI. Tenir à jour une cartographie détaillée et complète des SI. | **Oui** |
| ***4*** | **Gestion des biens** | Qualification et protection de l’information | Qualification et protection de l’information. Qualifier l’information de façon à adapter les mesures de protection. | **Oui** |
| ***5*** | **Intégration de la SSI dans le cycle de vie des systèmes d'information** | Gestion des risques et homologation de sécurité | Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d’information. | **Oui** |
| ***6*** | **Intégration de la SSI dans le cycle de vie des systèmes d'information** | Maintien en condition de sécurité des systèmes d’information | Maintien en condition de sécurité. Gérer dynamiquement les mesures de protection, tout au long de la vie du SI. | **Oui** |
| ***7*** | **Intégration de la SSI dans le cycle de vie des systèmes d'information** | Produits et services labellisés | Produits et services qualifiés ou certifiés. Utiliser des produits et services dont la sécurité est évaluée et attestée selon des procédures reconnues par l’ANSSI, afin de renforcer la protection des SI. | **Oui** |
| ***8*** | **Intégration de la SSI dans le cycle de vie des systèmes d'information** | Gestion des prestataires | Maîtrise des prestations. Veiller aux exigences de sécurité lorsqu’il est fait appel à de la prestation par des tiers. | **Oui** |
| ***9*** | **Sécurité Physique** | Sécurité physique des locaux abritant les SI Règles générales | Sécurité physique des locaux abritant les SI. Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés. | Non |
| ***10*** | **Sécurité physique** | Sécurité physique des centres informatiques | Sécurité physique des centres informatiques. Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités. | Non |
| ***11*** | **Sécurité physique** | SI de sûreté | Sécurité du SI de sûreté. Traiter de manière globale la sécurité des systèmes d’information et de communication qui assurent la sûreté d’un site. | Non |
| ***12*** | **Sécurité des réseaux** | Sécurité des réseaux nationaux | Usage sécurisé des réseaux nationaux. Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées. | **Oui** |
| ***13*** | **Sécurité des réseaux** | Sécurité des réseaux locaux | Usage sécurisé des réseaux locaux. Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs. | **Oui** |
| ***14*** | **Sécurité des réseaux** | Accès spécifiques | Accès spécifiques. Ne pas porter atteinte à la sécurité du SI par le déploiement d’accès non supervisés. | **Oui** |
| ***15*** | **Sécurité des réseaux** | Sécurité des réseaux sans fil | Usage sécurisé des réseaux sans fil. Maîtriser le déploiement, la configuration et l’usage des réseaux sans fil. | **Oui** |
| ***16*** | **Sécurité des réseaux** | Sécurisation des mécanismes de commutation et de routage | Sécurité des mécanismes de commutation et de routage. Configurer les mécanismes de commutation et de routage pour se protéger des attaques. | **Oui** |
| ***17*** | **Sécurité des réseaux** | Cartographie réseau | Cartographie réseau. Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions. | **Oui** |
| ***18*** | **Architecture des SI** | Architecture des centres informatiques | Architecture sécurisée des centres informatiques. Appliquer les principes de défense en profondeur à l’architecture matérielle et logicielle des centres informatiques. | **Oui** |
| ***19*** | **Exploitation des SI** | Protection des informations sensibles | Protection des informations sensibles. Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles. | **Oui** |
| ***20*** | **Exploitation des SI** | Sécurité des ressources informatiques | Surveillance et configuration des ressources informatiques. Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci. | **Oui** |
| ***21*** | **Exploitation des SI** | Gestion des autorisations et contrôle d’accès logique aux ressources | Autorisations et contrôles d’accès. Authentifier les usagers et contrôler leurs accès aux ressources des SI de l’État, en fonction d’une politique explicite d’autorisations. | **Oui** |
| ***22*** | **Exploitation des SI** | Exploitation sécurisée des ressources informatiques | Sécurisation de l’exploitation. Fournir aux administrateurs les outils nécessaires à l’exercice des tâches SSI et configurer ces outils de manière sécurisée. | **Oui** |
| ***23*** | **Exploitation des SI** | Défense des systèmes d’information | Défense des systèmes d’information. Défendre les SI nécessite une vigilance de tous, et des actions permanentes. | **Oui** |
| ***24*** | **Exploitation des SI** | Exploitation des centres informatiques | Exploitation sécurisée des centres informatiques. Exploiter de manière sécurisée les centres informatiques en s’appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision. | **Oui** |
| ***25*** | **Sécurité du poste de travail** | Sécurisation des postes de travail | Sécurisation des postes de travail. Durcir les configurations des postes de travail en protégeant les utilisateurs. | **Oui** |
| ***26*** | **Sécurité du poste de travail** | Sécurisation des imprimantes et copieurs multifonctions | Sécurisation des copieurs multifonctions. Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d’attaque. | **Oui** |
| ***27*** | **Sécurité du poste de travail** | Sécurisation de la téléphonie | Sécurisation de la téléphonie. Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes. | **Oui** |
| ***28*** | **Sécurité du poste de travail** | Contrôles de conformité | Contrôles de la conformité des postes de travail. Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail. | **Oui** |
| ***29*** | **Sécurité du développement des systèmes** | Développement des systèmes | Prise en compte de la sécurité dans le développement des SI. Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets. | **Oui** |
| ***30*** | **Sécurité du développement des systèmes** | Développements logiciels et sécurité | Prise en compte de la sécurité dans le développement des logiciels. Mener les développements logiciels selon une méthodologie de sécurisation du code produit. | **Oui** |
| ***31*** | **Sécurité du développement des systèmes** | Applications à risques | Sécurisation des applications à risques. Accompagner le développement sécurisé d’applications à risques par des contre-mesures minimisant l’impact d’attaques nouvelles. | **Oui** |
| ***32*** | **Traitements des incidents** | Chaînes opérationnelles | Chaînes opérationnelles. Partager l’information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques. | **Oui** |
| ***33*** | **Continuité d'activité** | Gestion de la continuité d’activité des SI | Gestion de la continuité d’activité. Se doter de plans de continuité d’activité, et les tester. | **Oui** |
| ***34*** | **Conformité, audit, inspection, contrôle** | Contrôles | Contrôles réguliers. Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements. | **Oui** |

## 2.4. Gestion des évolutions

(Procédure à renseigner)

# 3. Enjeux et objectifs de la SSI

## 3.1. Enjeux en matière de SSI

Identifier les enjeux de sécurité.

## 3.2. Objectifs en matière de SSI

Renseigner les objectifs de sécurité. Les objectifs de sécurité sont évalués selon les échelles DICT fournies dans la PSSI du MINISTERE de la JUSTICE.

# 4. Organisation de la SSI

## 4.1. Organisation de la cyber sécurité (Sécurité des Systèmes d’Information)

### 4.1.1. Chaîne décisionnelle de cyberdéfense (SSI)

Décrire l’organisation de la SSI du TITULAIRE (rôles et responsabilités). L’organisation doit être décrite au regard du contrat.

**RACI à intégrer**

# 5. Pilotage de la cyber sécurité

## 5.1. Cadre de référence appliqué

*EXEMPLE*

*L’adoption d’une démarche d’amélioration continue permet de :*

* *S’appuyer sur une norme internationale définissant le cadre des activités du domaine de la sécurité*
* *Assurer le pilotage de la sécurité par les risques dans le but de garantir l’efficience des activités et mesures de sécurité.*

*Selon la norme ISO 27001, le SMSI s'organise en quatre phases successives et cycliques (Planifier, Déployer, contrôler et Agir) permettant une amélioration continue du système.*

Cycle d’amélioration continue

## 5.2. Principes fondateurs

### 5.1.1. Assurer une amélioration continue

Dans la lignée du référentiel présenté ci-avant, Le MINISTÈRE DE LA JUSTICE retient le principe d’amélioration continue.

Cette amélioration continue passe par :

* Un processus d’améliorations concrètes réalisées dans un laps de temps court,
* Une standardisation des processus,
* Une adoption du principe par l’ensemble des acteurs,
* Une implication active du management pour le déploiement de la politique.

### 5.1.2. Analyser et traiter les risques

Les risques portant sur la sécurité du Système d’Information du MINISTÈRE DE LA JUSTICE constituent le point d’entrée des actions entreprises.

Le TITULAIRE doit réaliser une analyse des risques systématiques sur le SI dédié à la prestation.

Principes génériques de gestion des risques

* Les besoins de maîtrise des risques sont établis en évaluant l’impact potentiel de la réalisation d’un risque sur les intérêts du MINISTÈRE DE LA JUSTICE.
* Le porteur du risque est systématiquement identifié et le choix de la mesure de traitement est placé sous sa responsabilité. Les mesures de traitement des risques identifiées sont priorisées et mises en œuvre afin de diminuer la criticité des risques les plus forts pesant sur Le MINISTÈRE DE LA JUSTICE.
* *Les risques résiduels jugés critiques sont placés sous la surveillance du Contrôle Interne après acceptation ou refus du MINISTÈRE DE LA JUSTICE.*

### 5.1.3. Sensibiliser et former

Intégrer le plan de sensibilisation / formation des intervenants sur le SI du MINISTÈRE DE LA JUSTICE.

### 5.1.4. Réaliser la veille sécurité et réglementaire

Les activités de veille sont organisées à deux niveaux :

- la veille réglementaire qui a pour objectif de répondre au fort contexte législatif et normatif encadrant directement ou indirectement les activités du MINISTÈRE DE LA JUSTICE,

- la veille sécurité qui a pour objectif de gérer les vulnérabilités techniques sources de risques sur les actifs informationnels

-

**Veille réglementaire**

En regard des ensembles normatifs, réglementaires et contractuels du domaine, Le MINISTÈRE DE LA JUSTICE s’engage à mettre en place une veille réglementaire ayant pour objectif le respect du corpus qui lui est directement applicable,

**Veille Sécurité**

La veille sécurité est structurée autour de cinq sous-processus :

* assurer l’inventaire des actifs informatiques (c.f. inventaire xls),
* réaliser la veille technologique sécurité,
* cartographier les vulnérabilités logicielles existantes au sein du SI,
* identifier la ou les contre-mesures répondant aux situations de risque impliquées par une vulnérabilité logicielle,
* déployer et mettre en place la ou les contre-mesures adéquates.

### 5.1.5. Prévoir et gérer la réponse aux incidents de sécurité

Une organisation et des procédures de gestion des incidents sont formalisées.

Ces dernières ont pour vocation de :

* permettre une remontée efficace de tout défaut constaté par les utilisateurs du SI ou par les systèmes de détection et de supervision,
* garantir la réactivité et l’efficacité du processus global de résolution des incidents.

(à compléter)

### 5.1.6. Piloter la sécurité sur les bases d’indicateurs factuels et d’objectifs chiffrés

Insérer l’ensemble des indicateurs produit pour les Comités Sécurité (ou document de référence).

# 6. Responsabilités liées au PAS

Définir les responsabilités / les objectifs de sécurité et les pénalités associés en cas de défaillance du TITULAIRE.

# 7. Validation et diffusion

LE MINISTÈRE DE LA JUSTICE définit avec le client la liste des personnes concernées par le présent PAS.

Le tableau ci-dessous précise qui doit valider le Plan d’Assurance Sécurité et qui doit y avoir accès pour consultation.

\* Le PAS ne doit être diffusé qu’aux personnes habilitées à le recevoir, c’est-à-dire les personnes qui ont un besoin d’en connaître dans l’exercice de leur mission.

## 7.1. Procédure en cas de non-application et demande de dérogation

Un membre de l’équipe peut demander de déroger à une disposition prévue au PAS. Pour cela, il précisera par écrit le contenu, les limites, et le motif de sa demande et l’adressera au RSSI

*(A compléter)*

# 8. Procédures d’évolution du PAS

(Décrire les formalités contractuelles)

# 9. Mesures de sécurité appliquées

## 9.1. Ressources humaines

### 9.1.1. Avant l’embauche

Détailler le processus de recrutement ainsi que les enquêtes réalisées en conformités avec les exigences de sécurité.

### 9.1.2. Pendant la durée du contrat

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

## 9.2. Gestion des biens

### 9.2.1. Cartographie des SI

Un inventaire des biens du SI doit être réalisé à échéance régulière. Un propriétaire (personne faisant autorité sur le bien, en fonction des données hébergées) doit être défini pour chaque bien. Le terme de propriétaire est entendu au sens fonctionnel.

### 9.2.2. Qualification et protection de l’information

Les biens sont qualifiés en termes de sécurité selon les critères de DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité). Le niveau attribué à chaque bien permet de définir les moyens de sécurité adaptés.

Les critères sont définis comme suit :

* Disponibilité : Propriété d'accessibilité au moment voulu des biens essentiels,
* Intégrité : Propriété d'exactitude et de complétude des biens essentiels,
* Confidentialité : Propriété des biens de n'être accessibles qu'aux utilisateurs autorisés,
* Traçabilité : Propriété permettant aux biens de générer des traces des opérations effectuées.

## 9.3. Intégration de la SSI dans le cycle de vie des systèmes d'information

### 9.3.1. Gestion des risques et homologation de sécurité

### 9.3.2. Maintien en condition de sécurité des systèmes d’information

### 9.3.3. Produits et services labellisés

LE MINISTÈRE DE LA JUSTICE n’est pas éditeur de produits informatiques et les services rendus par Le MINISTÈRE DE LA JUSTICE ne nécessitent aucune labélisation.

Dans le même temps et en conformité avec la PSSIE, Le MINISTÈRE DE LA JUSTICE s’engage à utiliser des produits de sécurité faisant l’objet d’une validation de l’ANSSI.

Le TITULAIRE s’engage à n’utiliser que des services labellisés au regard des exigences de sécurité. Le titulaire s’engage à fournir au MINISTÈRE DE LA JUSTICE une liste exhaustive des services utilisés sur le périmètre du contrat.

### 9.3.4. Gestion des prestataires

## 9.4. Sécurité Physique

***A renseigner en fonction du contrat.***

## 9.5. Sécurité des réseaux

Afin de garantir la sécurité des informations, des zones de sécurité logique sont définies. Ces zones sont cloisonnées du reste du SI.

Des infrastructures garantissent le filtrage des flux avec tout réseau externe.

Les serveurs sont hébergés dans des zones de sécurité dédiées. Ils sont installés et configurés afin de ne proposer que les services strictement nécessaires.

Tous les accès internet sont connus et maîtrisés. Les accès internet ne respectant pas les règles et les spécifications techniques standards font l’objet d’une dérogation motivée.

Une procédure de gestion des flux est écrite. Un corpus de règles de filtrage existe et tous flux ne respectant pas ces règles doivent faire l’objet d’une dérogation motivée.

### 9.5.1. Sécurité des réseaux nationaux (sécurisation des flux)

Les échanges d’informations en interne, au sein du MINISTÈRE DE LA JUSTICE ou avec des tiers doivent s’effectuer en accord avec leur niveau de classification, en particulier en matière de confidentialité.

En parallèle, comme précisé dans Charte d’usage des services numériques du MINISTÈRE DE LA JUSTICE, les utilisateurs doivent être vigilants quant à la transmission d’information par mail ou au travers du web. Ses règles visent notamment à lutter contre :

* la propagation de codes malveillants,
* l’interception d’informations sensibles,
* la désinformation,
* la publication d’informations pouvant nuire à Le MINISTÈRE DE LA JUSTICE.

Les informations considérées selon la classification du MINISTÈRE DE LA JUSTICE comme sensibles ne peuvent être transmises via l’infrastructure et services standards du MINISTÈRE DE LA JUSTICE. Ces informations ne pourront pas être envoyées par l’email standard du MINISTÈRE DE LA JUSTICE. Elles devront obligatoirement être transmises via un système de sécurité validé par le RSSI.

### 9.5.2. Sécurité des réseaux locaux

### 9.5.3. Accès spécifiques

### 9.5.4. Sécurité des réseaux sans fil

### 9.5.5. Sécurisation des mécanismes de commutation et de routage

### 9.5.6. Cartographie réseau

## 9.6. Architecture des SI

### 9.6.1. Architecture des centres informatiques

## 9.7. Exploitation des SI

### 9.7.1. Protection des informations sensibles

Les données sensibles type données à caractère personnel ne doivent être exploitées que pour des traitements légitimes. Les finalités doivent être licites et justifiées.

Toutes les données dites sensibles devront être chiffrées avant transmission à un tiers légitime.

Les données devront également être chiffrées sur les disques si les machines sont exposées physiquement.

### 9.7.2. Sécurité des ressources informatiques

Les exigences métiers s’inscrivent dans la logique du moindre privilège. Selon le principe du moindre privilège, les utilisateurs se voient attribuer un niveau d’habilitation qui correspond exactement à leur mission.

### 9.7.3. Gestion des autorisations et contrôle d’accès logique aux ressources

La gestion de la création des comptes est expliquée dans la partie liée aux ressources humaines.

### 9.7.4. Exploitation sécurisée des ressources informatiques

Les responsabilités liées à l’exploitation sont définies et formalisées. Les principes de séparation des pouvoirs sont appliqués pour réduire les risques d’erreur ou de malveillance. En cas de cumul des pouvoirs, des mesures conservatoires sont prises afin de garantir notamment une meilleure traçabilité des actions.

Tous les systèmes sont régulièrement maintenus à jour afin d’intégrer les derniers correctifs fonctionnels et de sécurité :

- les correctifs comblant des vulnérabilités critiques – c’est-à-dire pouvant conduire à l’exécution de code arbitraire ou la prise de main à distance – sont déployés dans les plus brefs délais,

- les autres correctifs sont déployés à intervalles réguliers.

Préalablement au déploiement, chaque correctif fait l’objet d’une analyse des effets possibles en cas d’application et de non application. Les résultats de cette analyse déclenchent la mise en production ou non. Lorsqu’un correctif n’est pas déployé, une justification est fournie au RSSI.

### 9.7.5. Défense des systèmes d’information

### 9.7.6. Exploitation des centres informatiques

## 9.8. Sécurité du poste de travail

### 9.8.1. Sécurisation des postes de travail

### 9.8.2. Sécurisation des imprimantes et copieurs multifonctions

### 9.8.3. Sécurisation de la téléphonie

### 9.8.4. Contrôles de conformité

## 9.9. Sécurité du développement des systèmes

***A renseigner en fonction du contrat***

## 9.10. Traitements des incidents

Un incident de sécurité est un évènement de sécurité ayant provoqué une violation avérée de la sécurité.

### 9.10.1. Chaînes opérationnelles

Le processus de gestion des incidents de sécurité est décrit dans le document de référence (processus de gestion des incidents de sécurité).

Des fiches réflexes sont associées au processus de gestion des incidents afin d’obtenir une réponse sur incidents adaptés à plusieurs cas de figure et donc plus efficaces.

## 9.11. Continuité d'activité

### 9.11.1. Gestion de la continuité d’activité des SI

(Description des PCA et PRA)

## 9.12. Conformité, audit, inspection, contrôle

La mise en œuvre d’une gestion de la conformité, aux exigences légales et règlementaires, mais également à la PSSI du Ministère de la Justice est un élément essentiel au pilotage de la démarche sécurité. La démarche associée est précisée ci-dessous.

### 9.12.1. Conformité avec les exigences légales et règlementaires

Les obligations légales et réglementaires doivent être respectées par les directions, et en particulier celles découlant des législations françaises, mais également européennes.

Les obligations légales et règlementaires spécifiques à la protection de l’information doivent être respectées.

### 9.12.2. Conformité avec les politiques de sécurité

La sécurité du système d’information n’est effective que si les principes de sécurité sont appliqués.

Tous les utilisateurs doivent s’assurer que les procédures de sécurité sont correctement appliquées dans leurs domaines d’activité. A ce titre, les utilisateurs doivent respecter la Charte d’usage des services numériques du MINISTÈRE DE LA JUSTICE.

### 9.12.3. Revue de la sécurité de l’information

Des revues régulières doivent être effectuées pour s’assurer que les politiques de sécurité sont respectées.

Des contrôles réguliers et des revues de la conformité du système d’information aux politiques de sécurité doivent être effectués. Ces contrôles, formalisés dans un plan de contrôle, incluent toutes les mesures nécessaires à la vérification de la sécurité des équipements et des logiciels : test des systèmes d’exploitation, test des logiciels, test d’intrusion…

### 9.12.4. Contrôles

Pour chaque règle de la PSSI Le MINISTÈRE DE LA JUSTICE propose des contrôles. Une matrice de contrôle par règle ou exigence de la PSSI est produite et mise à jour par Le MINISTÈRE DE LA JUSTICE.

LE MINISTÈRE DE LA JUSTICE s’autorise à réaliser un audit de la sécurité du SI du prestataire par an.

# 10. Couverture des exigences de sécurité

(Résultats de l’auto-évaluation avec l’outil excel)