

Obligations du titulaire en matière de sécurité des systèmes d'information

Date d'application : 01/09/2019

Version : V1.0

Retrouvez-nous sur :
justice.gouv.fr

Circuit de validation

Date application	Version	Objet	Rédaction	Vérification	Approbation
01/09/2019	V1.0	Sécurité des systèmes d'information	20/08/2019 Dominique PAILHAREY	01/09/2019 Edouard SLOTTJE	01/09/2019 Edouard SLOTTJE

Diffusion

Pour action	
Pour information	

Historique des modifications

Date application	Version	Objet	Rédaction	Vérification	Approbation
jj/mm/aaaa	Vx.y (VPxx)		jj/mm/aaaa <Nom>	jj/mm/aaaa <Nom>	jj/mm/aaaa <Nom>

Sommaire

1	Objet.....	3
2	Domaine d'application	3
3	Références, définitions et terminologie	3
3.1	Documents de référence.....	3
3.2	Définitions.....	3
3.3	Terminologie.....	4
4	Obligations du titulaire	4
4.1	Etat de l'art.....	4
4.2	Obligations du titulaire en termes de sécurité	4
4.3	Plan d'Assurance Sécurité.....	5
4.4	Gouvernance sécurité du titulaire	5
4.5	Gestion de crise.....	5
4.6	Localisation des données	6
4.7	Sécurité Physique.....	6
4.8	Gestion des biens.....	7
4.9	Qualifications ANSSI.....	8
4.10	Développement sécurisé.....	8
4.11	Protection du code source	9
4.12	Analyse virale des documents en entrée	9
4.13	Sécurité du poste de travail	9
4.14	Obligation pour les titulaires intervenant au sein des locaux du ministère	9
4.15	Interconnexion des Sis du ministère et du titulaire	10
4.16	Obligations spécifiques liées aux prestation d'étude.....	10
4.17	Politique d'exploitation des environnements du titulaire.....	10
4.18	Disponibilité des données	12
4.19	Continuité et reprise d'activité.....	12
4.20	Documentation relative aux applications.....	12
4.21	Réversibilité des applications	13

1 Objet

En matière de sécurités des systèmes d'information, les principaux risques identifiés sont les suivants :

- Intrusion volontaire ou non sur les systèmes d'information du Ministère de la Justice par un agent du titulaire ou en utilisant les installations du titulaire ;
- Détournement volontaire de données et/ou de leur flux, par un agent du titulaire ou en utilisant les installations du titulaire ;
- Non-respect par le titulaire des bonnes pratiques de développement sécurisé entraînant l'introduction de failles de sécurité dans le code de l'application ;
- Diffusion de données sensibles.

Les exigences et clauses de sécurité listées dans ce document visent à réduire ces risques à un niveau acceptable.

Le titulaire doit s'y conformer.

2 Domaine d'application

Ce document a vocation à être annexé aux CCTP publiés par le ministère.

3 Références, définitions et terminologie

3.1 Documents de référence

Référence	Version	Titre
http://circulaire.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&retourAccueil=1&r=39217		Instruction interministérielle relative à la protection des Systèmes d'Information sensibles n° 901/SGDSN/ANSSI (NOR : PRMD1503279J)
https://www.owasp.org		OWASP (Open Web Application Security Project)
https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/	version 2.0 ou supérieure	Référentiel Général de Sécurité (RGS) de l'ANSSI (Agence nationale de sécurité des systèmes d'information)
http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-interministerielle-n-901/		L'instruction interministérielle N°901 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR)
http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/		La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf		Les guides de bonnes pratiques de la CNIL pour la protection des données à caractère personnel

3.2 Définitions

Terme	Définition

3.3 Terminologie

Acronyme	Définition
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
CCTP	Cahier des Clauses Techniques Particulières
PAS	Plan d'Assurance Sécurité
RGS	Référentiel Général de Sécurité

4 Obligations du titulaire

4.1 Etat de l'art

Le titulaire conçoit, met en œuvre et exploite les systèmes d'informations sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière. Toutefois, il doit respecter les exigences suivantes pour les services Web et de messagerie :

- Interfaces web :
 - o Les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.) ou une technologie en particulier ;
 - o Les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications ; l'utilisation de la technologie HSTS est fortement recommandée ;
 - o Les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
 - o Une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;
 - o Les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés.
- Services de courriels :
 - o Les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) ;
 - o La mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout (DMARC).

4.2 Obligations du titulaire en termes de sécurité

Le titulaire est tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité. En particulier, il informe le Ministère de la Justice des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Le titulaire est responsable du maintien en condition de sécurité du système (MCS) de ses environnements pendant toute la durée des prestations.

Le titulaire met en œuvre sur ses environnements le même niveau de protection des données que celui imposé par la réglementation au sein du Ministère de la Justice. Le document de référence est communiqué au Responsable Sécurité Opérationnelle du titulaire dès lors qu'il a fait la preuve qu'il peut consulter des documents de diffusion restreinte.

4.3 Plan d'Assurance Sécurité

Le titulaire applique et fait appliquer à ses sous-traitants la politique de sécurité du présent marché. Cette politique de sécurité traite notamment des thèmes suivants :

- Organisation de la Sécurité des SI ;
- Application de la Politique de Sécurité des SI ;
- Évaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI : réseaux, systèmes ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;
- Développement et maintenance des systèmes ;
- Gestion des incidents et des alertes ;
- Gestion de la continuité d'activité des SI ;
- Conformité et démarche de contrôle interne ;
- Localisation des données.

Le titulaire exécute ses obligations en termes de sécurité des systèmes d'information. À ce titre, il décrit dans le cadre d'un Plan d'Assurance Sécurité (PAS) les mesures qu'il met en œuvre pour se conformer aux exigences de sécurité décrites ci-après ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité du donneur d'ordres pendant toute la durée des prestations.

4.4 Gouvernance sécurité du titulaire

Afin de garantir la bonne prise en compte de la sécurité par le titulaire, il est important que celui-ci dispose d'une gouvernance sécurité et que celle-ci soit conforme aux exigences du Ministère de la Justice.

Le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.

Le titulaire met à disposition du Ministère de la Justice les politiques et procédures de sécurité mises en œuvre pour assurer la bonne prise en compte de la sécurité, dans le respect des demandes formulées par le Ministère de la Justice.

Le titulaire identifie au sein de ses équipes, un Responsable Sécurité Opérationnelle qui est l'interlocuteur privilégié du Ministère de la Justice dans le cadre de cette gouvernance sécurité.

Cet interlocuteur est notamment :

- L'interlocuteur privilégié de l'administration pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'administration ou le titulaire suite à des incidents de sécurité opérationnels ;
- Chargé du maintien et de la mise en application du PAS.)
- Joignable aux du lundi au vendredi 9H30-18H00. Tout remplacement de ce correspondant doit être notifié à l'administration conformément à l'article VI.5 du CCAP. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

Le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.

Le titulaire met à disposition du Ministère de la Justice les politiques et procédures de sécurité mises en œuvre pour assurer la bonne prise en compte de la sécurité, dans le respect des demandes formulées par le Ministère de la Justice.

4.5 Gestion de crise

Sur son domaine de responsabilité SI, le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'administration le respect des engagements de service et de sécurité SI contractualisés.

Ce plan précise au minimum :

- Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- La composition de la cellule de crise : fonctions et responsabilités des membres (administration 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).

4.6 Localisation des données

Le titulaire communique au Ministère de la Justice la liste de tous les lieux de stockage de données détenues dans le cadre du présent accord-cadre sur tout type d'environnement tels que les environnements de développement, d'intégration, de maintenance, de recette, ...

De plus, dans le cas de données à caractère personnel, les lieux d'hébergement doivent également satisfaire aux dispositions de la loi du 6 janvier 1978 modifiée relative à la protection des données à caractère personnel.

Conformément à l'Instruction interministérielle relative à la protection des Systèmes d'Information sensibles n° 901/SGDSN/ANSSI (NOR : PRMD1503279J), l'hébergement des données sensibles du Ministère de la Justice sur le territoire national est obligatoire.

4.7 Sécurité Physique

- **Changement de localisation géographique des services et des données :** En cas de changement de localisation des données ou services, le titulaire en informe préalablement l'administration.
- **Hébergement de données :** À première demande de l'administration, le titulaire identifie tous les titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.
- **Contrôle d'accès physique aux bâtiments du titulaire :** les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire.

Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.

- **Contrôle des accès aux ressources techniques du titulaire :** le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'administration et les équipements de sûreté.

- **Protection intrusion physique des locaux techniques du titulaire :** les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :
 1. Protection contre l'intrusion et les effractions ;
 2. Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
 3. Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction.

En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

- **Accompagnement des visiteurs :** le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.

- **Protection des plateaux mutualisés :** en cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'administration (accès au poste

par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'administration, etc.).

- **Étanchéité physique des ressources informatiques :** les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la prestation de l'administration n'a pas de murs adjacents à d'autres bureaux.

Le titulaire met en place des moyens garantissant une étanchéité physique entre les infrastructures physiques dédiées à l'administration de celles des autres clients au sein des salles informatiques.

- **La salle hébergeant des matériels de l'administration doit si possible lui être dédiée ;**

Dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'administration une solution de « suite privative » au sein de la salle multi-clients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

4.8 Gestion des biens

- **Séparation des données de l'administration et des données d'autres clients :** le titulaire conserve et traite les données de l'administration de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de l'administration suivant le principe de restriction au besoin d'en connaître.
- **Protection de la documentation de l'administration sur support papier :** le titulaire assure la protection de la documentation de l'administration sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.
- **Modalités d'échanges d'informations :** le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.
- **Echanges de supports :** le titulaire garantit que les supports échangés ou à connecter sur un SI de l'administration n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'administration.
- **Transmission de fichiers sur un support physique :** toute transmission de fichiers sur un support physique (DAT, CDRom, etc.), par courrier externe ou par porteur, donne lieu à un accusé de réception.

Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'administration.

De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

- o L'émetteur et le destinataire;
- o Le détail des opérations de transferts et notamment le nombre et la date.

Sur simple demande, ce registre est mis à la disposition de l'administration adjudicateur par le titulaire.

- **Marquage des ressources techniques :** Le titulaire applique des règles de marquage 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 ou classifiées.
- **Supports de stockage hébergeant des données de l'administration :** le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données de l'administration, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'administration.

- **Maintien à jour et mise à disposition des données relatives à la prestation :** le titulaire maintient à jour et est en mesure de mettre à disposition de l'administration toutes les données relatives à la prestation.

Le titulaire fournit systématiquement toute la documentation générée dans le cadre de la prestation à l'administration pour archive.

4.9 Qualifications ANSSI

Chaque fois que cela sera possible le titulaire s'emploiera à utiliser des équipements et ou des logiciels labélisés par l'ANSSI (certificat, qualification, attestation, visas de sécurité, ...). Dans les cas contraires, le titulaire proposera des équipements et/ou logiciels ayant des labels équivalents.

4.10 Développement sécurisé

Le titulaire met en place des mesures permettant d'assurer la production d'un code source applicatif sécurisé. Ces mesures incluent notamment :

- La sensibilisation des développeurs au respect des règles et bonnes pratiques de sécurité : OWASP, guides de l'ANSSI en particulier le Référentiel Général de Sécurité (RGS) de l'ANSSI (Agence nationale de sécurité des systèmes d'information) version 2.0 ou supérieure, etc.
- L'intégration de contrôles et audits de la sécurité du code tout au long de son train de maintenance de développement.
- La prise en compte des recommandations formulées dans le cadre d'audits de sécurité et de tests d'intrusion commandités par le titulaire ou le Ministère de la Justice.
- L'utilisation du cadre standard de développement : le titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) de l'administration comprenant notamment :
 - o l'organisation des équipes de développement et de la prestation ;
 - o les configurations matérielles préconisées pour le développement ;
 - o les outils de développement préconisés par l'administration (logiciels, versions, etc.) ;
 - o une structure de développement (framework) intégrant les fonctions de sécurité.
- La ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.
- La traçabilité des actions de développement : toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure.
- La conduite des tests : lors de la conduite de tests de validation ou du déploiement, le titulaire doit :
 - o utiliser des données de tests anonymisées ;
 - o ne pas provoquer de perturbations du système d'information de l'administration lors des séances de test ;
 - o remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible
 - o ne pas introduire de régression vis-à-vis d'un état de sécurité atteint dans une version précédente

Ces mesures doivent être décrites dans le Plan d'Assurance Sécurité et pouvoir être contrôlées.

4.11 Protection du code source

Le titulaire met en place des mesures de protection de l'intégrité du code source durant l'intégralité de la durée de l'accord-cadre. Il doit également assurer :

- La traçabilité des modifications apportées au code source ;
- Un contrôle strict des personnes autorisées à accéder au code source, dans le respect du principe du droit d'en connaître.
- La Sauvegarde des codes sources : le titulaire doit sauvegarder et conserver chaque version du code source recettée dans le cadre de la prestation. Les accès à ces sauvegardes devront être tracés.
- Le Dépôt des codes source : le titulaire doit déposer les codes sources dans ses différentes versions et mises à jour selon les recommandations de l'administration.

Le titulaire doit assurer la disponibilité du code source, notamment par une politique de sauvegarde régulière et un plan de restauration des données en cas de sinistre.

Par ailleurs, à la demande du Ministère de la Justice, le titulaire met à disposition une copie intégrale du code source et de la documentation projet associée.

4.12 Analyse virale des documents en entrée

L'ensemble des documents et données entrants dans le système d'information sont contrôlés par un anti-virus dans le cadre des processus de versement.

Le Ministère de la Justice utilise l'anti-virus SOPHOS sur lequel le titulaire a la possibilité de s'appuyer.

4.13 Sécurité du poste de travail

Le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivols de façon systématique.

Une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

4.14 Obligation pour les titulaires intervenant au sein des locaux du ministère

- Respect des exigences de sécurité de l'administration : au même titre que les agents de l'administration, le titulaire doit prendre connaissance et appliquer les règlements internes de l'administration (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).
- Respect des standards et méthodologies de l'administration : le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'administration.
- Respect du périmètre de la prestation : le titulaire ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.
- Connexion d'équipements au réseau de l'administration : le titulaire doit connecter sur le réseau interne de l'administration uniquement des équipements fournis par l'administration. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, etc.).
- Inventaire des composants mis à disposition par l'administration : le titulaire met en place une solution pour élaborer et maintenir un inventaire complet et à jour des composants mis à disposition par l'administration. Cette liste devra être transmise régulièrement à l'administration
- Recensement des comptes d'accès : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'administration existants ainsi que des rôles et privilèges qui y sont associés.

Il doit être en mesure de fournir cette liste à l'administration sur demande.

Le titulaire doit également effectuer et formaliser :

- o une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la Prestation ;
- o une revue « d'emploi » (*a minima* trimestrielle), une revue de « besoin » (*a minima* annuelle).
- Restitution des équipements fournis par l'administration : à la fin de la prestation, le titulaire doit restituer l'ensemble du matériel fourni par l'administration .

- Restitution des informations collectées par le titulaire : à la fin de la prestation, le titulaire doit restituer ou détruire les informations de l'administration en sa possession. Un procès-verbal de destruction des données doit être signé par le titulaire conformément aux dispositions de l'article VI.6 du CCAP.
- Transfert de connaissances : le titulaire doit préciser la date exacte de départ des intervenants de la prestation et organiser le transfert de connaissances auprès des équipes de l'administration.

4.15 Interconnexion des Sis du ministère et du titulaire

- Respect des exigences de sécurité de l'administration : au même titre que les agents de l'administration, le titulaire prend connaissance et applique les règlements internes de l'administration (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).
- Respect des standards et méthodologies de l'administration : le titulaire respecte les standards et les méthodologies préconisés au sein de l'administration et figurant en annexe du présent CCTP.
- Respect du périmètre de la prestation : le titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.
- Interconnexion des SI de l'administration et du titulaire : en cas d'interconnexion des SI de l'administration et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'administration au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'administration.

Pour chaque interconnexion, les éléments suivants doivent être définis :

- les flux et protocoles autorisés, ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ;
- les modalités d'authentification requises : authentification par mot de passe, authentification forte par mot de passe unique ou par certificat ;
- les modalités de chiffrement des échanges : le chiffrement des flux transitant sur Internet est requis ;
- les exigences spécifiques de traçabilité des accès ;
- les moyens de sécurité supplémentaires à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif.

4.16 Obligations spécifiques liées aux prestation d'étude

- Respect des standards et méthodologies de l'administration : le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'administration. En particulier, le titulaire doit appliquer les méthodes d'évaluation de la sensibilité et d'analyse de risques des systèmes d'information lorsqu'il intervient dans les phases amont des projets.
- Ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.
- Conduite des tests : lors de la conduite de tests de validation ou du déploiement, le titulaire doit :
 - o utiliser des données de tests anonymisées (sauf accord explicite de l'administration) ;
 - o ne pas provoquer de perturbations du système d'information de l'administration lors des séances de test ;
 - o remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible.

4.17 Politique d'exploitation des environnements du titulaire

Le titulaire met en œuvre :

- Une politique d'exploitation sur ses environnements (postes de travail, serveurs développement et de recette, réseaux, applicatifs, etc.) :
 - o Gestion des changements ;
 - o Sauvegarde et restauration ;
 - o Supervision.
- Les procédures opérationnelles associées

Le titulaire propose le sommaire de ces documents dans le Plan d'Assurance Sécurité (Le Ministère de la Justice se réserve le droit de contrôler éventuellement le contenu de cette documentation).

- Cloisonnement des environnements informatique: le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation. Le niveau d'engagement de disponibilité de ses environnements sont décrits dans le Plan d'Assurance Sécurité et peuvent être contrôlés et audités régulièrement par le Ministère de la Justice.
- Sécurisation des flux d'administration: le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni à aux infrastructures bureautique du titulaire.
- Règles de sécurité et d'exploitation : l'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'administration. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'administration.
- Anti-virus opérationnel et à jour : le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation.
- La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à l'administration.
- Gestion des mises à jour : le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirus, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'administration.
- Sauvegarde des données : le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergée sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés par le chef de projet de l'administration dans le cadre de la Prestation.
- Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.
- Stockage des sauvegardes informatiques : le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.
- Comptes individuels¹ : le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez l'administration) dispose d'un compte individuel qui peut être :
 - o Soit un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte ;
 - o Soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.
- Comptes obsolètes ou par défaut : le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.
- Comptes techniques : dans le cadre de la cartographie du système d'information prévue à l'article VI.4 du CCAP, le titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.
- Recensement des comptes d'accès : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'administration existants ainsi que des rôles et privilèges qui y sont associés.
- Il fournit cette liste à l'administration sur demande.
- Le titulaire effectue et formalise :
 - o une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.
 - o une revue « d'emploi » (a minima trimestrielle), une revue de « besoin » (a minima annuelle).
- Politique du moindre privilège² : le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.
- Attaques en essai et erreurs sur secrets d'authentification : les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai

¹ Les comptes concernés par cette exigence sont bien ceux gérés par le titulaire.

² Le principe du moindre privilège est le principe selon lequel chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches.

et erreur sur les secrets d'authentification³.

- Journalisation des actions : le titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves.

Le titulaire collecte et stocke à minima les informations suivantes :

- o Connexion et déconnexion aux équipements et applications ;
- o Consultations d'informations relatives à la vie privée ;
- o Informations d'usage de l'Internet (accès aux sites Web) ;
- o Accès en lecture et/ou en écriture à des fichiers et dossiers marqués « CONFIDENTIEL » ;
- o Informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

- Gestion des traces : le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, diverses dates liées aux fichiers, clés de registres...). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.
- Politique de mot de passe : le titulaire respecte la politique de définition des mots de passe de l'administration⁴ sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.
- Sources d'installation des logiciels : le titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par l'administration.
- Validité des licences : le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'administration dans le cadre de la prestation.

4.18 Disponibilité des données

Durant le marché, le titulaire maintient la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information dans un délai maximum d'une semaine.

En cas de non-respect de ces délais, l'administration applique les pénalités visées à l'article XI.3.1 du CCAP.

4.19 Continuité et reprise d'activité

Le titulaire dispose d'un plan de continuité et de reprise d'activité. Ce dernier décrit les mesures organisationnelles et techniques mises en œuvre par le titulaire pour assurer la continuité de ses activités en cas de sinistre sur les ressources allouées à la réalisation du présent accord-cadre.

- Plan de continuité d'activité : le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat dans les délais maximum d'une semaine. Il fournit, à la demande de l'administration, la preuve de l'existence d'un plan de continuité d'activité régulièrement testé pour l'ensemble des services fournis à l'administration. L'administration se réserve le droit de demander les résultats des exercices de continuité d'activité réalisés régulièrement par le titulaire.
- Incident affectant la continuité des services : En cas d'incident affectant la continuité des services, le titulaire signale l'événement à l'administration selon la procédure d'alerte qu'il a définie à l'article 4.4.1 du CCTP « gestion des incidents de sécurité sur les environnements du titulaire ».

4.20 Documentation relative aux applications

Dans un souci de bonne utilisation des applications et de traçabilité, le Ministère de la justice dispose d'une copie de toutes les informations et documents relatifs au train de maintenance de vie des applications.

³ Exemple de mesure de protection : blocage pendant 30 minutes de la session d'un poste de travail après 3 tentatives de connexion échouées.

⁴ Cf le guide correspondant : <https://www.ssi.gouv.fr/guide/mot-de-passe/>

4.21 Réversibilité des applications

Le titulaire prévoit les modalités de récupération de données. En particulier, le titulaire fournit au Ministère de la justice une procédure de récupération de données dans un format exploitable et dans leur dernière version. Les données restituées doivent être complètes, fiables et intègres.