



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

**DIRECTION DE L'ÉVALUATION DE LA PERFORMANCE, DE L'ACHAT, DES FINANCES ET DE
L'IMMOBILIER**

**SERVICE ACHAT INNOVATION LOGISTIQUE DU MINISTÈRE DE L'INTÉRIEUR
SOUS-DIRECTION DE L'ACHAT ET DU SUIVI DE L'EXÉCUTION DES MARCHÉS
BUREAU DES ACHATS IMMOBILIERS ET PRESTATIONS**

ANNEXE 1

PROTECTION DES INFORMATIONS – CONFIDENTIALITE – MESURES DE SECURITE

1. GENERALITES.....	3
2. REFERENCE AU CCAG.....	3
3. MESURE DE SECURITE APPLICABLES A L'ACCES AUX LOCAUX.....	3
4. EXIGENCES ADMINISTRATIVES APPLICABLES AUX SYSTEMES D'INFORMATION	4
4.1 PLAN D'ASSURANCE SECURITE.....	4
4.2 HEBERGEMENT DES DONNEES ET DES SERVICES.....	4
4.1 CONSEIL ET DE CONFORMITE A L'ETAT DE L'ART.....	5
4.3 CARTOGRAPHIE DES SYSTEMES D'INFORMATION	5
4.4 PROTECTION DE L'INFORMATION.....	5
4.5 MAINTIEN EN CONDITION DE SECURITE.....	6
4.6 INFORMATION SUR LES EVENEMENTS ET INCIDENTS DE SECURITE.....	6
4.7 SECURISATION DES LOCAUX DU TITULAIRE.....	7
4.8 ECHEANCE OU RESILIATION DU MARCHE.....	7
4.9 AUDIT DE SECURITE SUR LE PERIMETRE DU TITULAIRE.....	8
5. EXIGENCES TECHNIQUES APPLICABLES AUX SYSTEMES D'INFORMATION	8
5.1 PROCESSUS D'HOMOLOGATION DES SI.....	8
5.2 MAINTIEN EN CONDITION DE SECURITE.....	10
5.3 ETAT DE L'ART.....	13
5.4 GESTION DES BIENS DE L'ACHETEUR.....	14
5.5 SECURITE DE SES LOCAUX INFORMATIQUES.....	15
5.6 SECURITE DES RESEAUX ET DE L'EXPLOITATION	17
5.7 SECURITE DE SES POSTES DE TRAVAIL	19
5.8 TRAITEMENT DES INCIDENTS DE SECURITE.....	20
5.9 ACCES AUX LOCAUX DE L'ACHETEUR.....	20
5.10 INTERVENTION AU SEIN DES LOCAUX DE L'ACHETEUR.....	21
5.11 NOMADISME NUMERIQUE	21
5.12 INTERCONNEXION AVEC LES SI DU TITULAIRE.....	22
5.13 PRESTATIONS D'ETUDE.....	22
5.14 SECURITE DES DEVELOPPEMENTS.....	23
5.15 ACHATS DE SERVICES, MATERIELS OU LOGICIELS	26
5.16 GESTION DES DROITS D'ACCES	27
5.17 GESTION DES PERSONNELS	28
5.18 CONTINUITE D'ACTIVITE.....	28
6. PROTECTION DES INFORMATIONS SENSIBLES	29
6.1 PRINCIPES	29
6.2 PROTECTION DES INFORMATIONS SENSIBLES SUR SUPPORT PAPIER.....	30
6.3 PROTECTION DES INFORMATIONS SENSIBLES SUR SUPPORT ELECTRONIQUE.....	30
6.4 SECURISATION DES LOCAUX DU TITULAIRE	31

1. GENERALITES

Dans la présente annexe, les dispositions relatives aux sous-traitants ne valent que dans les cas où la sous-traitance est autorisée par le marché. De la même façon, les dispositions relatives au support ou à la maintenance ne valent que si ces prestations sont prévues au marché.

2. REFERENCE AU CCAG

Le titulaire est tenu de respecter les obligations de confidentialité, de protection des données à caractère personnel et les mesures de sécurité prévues à l'article 5 du CCAG applicable au marché contractualisé.

Si un sous-traitant est susceptible d'intervenir pour le compte du titulaire durant l'exécution de l'accord-cadre, le titulaire est tenu de l'aviser de ce que ces obligations lui sont applicables.

Quel que puisse être le statut de ce sous-traitant vis-à-vis du titulaire, ce dernier reste responsable du respect de ces obligations.

3. MESURE DE SECURITE APPLICABLES A L'ACCES AUX LOCAUX

Tout agent du titulaire, que celui-ci soit l'un de ses salariés ou salarié d'un de ses sous-traitants, devant avoir accès aux locaux de l'administration doit être préalablement nommé agréé selon la procédure en vigueur au ministère de l'intérieur (MI).

Cet agent du titulaire demeure soumis pendant son séjour aux mêmes règles intérieures que les agents de l'administration, notamment les politiques et procédures de sécurité des systèmes d'information, ainsi que les chartes administrateurs et utilisateurs.

Le ministère de l'intérieur peut retirer son agrément à tout moment sans avoir à énoncer ses motifs, le titulaire doit alors proposer immédiatement un remplaçant de niveau équivalent.

L'intervention dans les locaux de l'administration est conditionnée à l'obtention d'une autorisation d'accès délivrée à l'agent du titulaire après enquête diligentée par le service de sécurité compétent pour l'autorité contractante au profit de laquelle le marché est exécuté.

Le délai d'enquête est en moyenne de quinze (15) jours ouvrés et il est fait obligation au titulaire de fournir à l'administration :

- le patronyme et les prénoms de son agent ;
- une photocopie lisible et recto-verso d'un titre d'identité dont la nature varie selon la situation individuelle de l'agent visé :
 - carte nationale d'identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires ;
 - titre de séjour en cours de validité avec autorisation de travail préalable ou carte de résident pour les étrangers extracommunautaires ;
- l'adresse actuelle de l'agent si celle-ci diffère de celle portée sur le titre d'identité fourni.

4. EXIGENCES ADMINISTRATIVES APPLICABLES AUX SYSTEMES D'INFORMATION

4.1 Plan d'Assurance Sécurité

La structure du PAS doit reprendre, a minima, l'ensemble des chapitres de la norme ISO 27002:2013. La mention « Sans Objet » devra être inscrite sous chaque chapitre ou partie non applicable.

Le Titulaire doit veiller à ce que les exigences définies dans son PAS soient conformes aux exigences de sécurité applicables de la PGSN du ministère de l'Intérieur, durant toute la durée du marché. A ce titre, le PAS doit également inclure une matrice de conformité aux exigences de la Politique générale de sécurité numérique du ministère de l'Intérieur.

La PGSN du ministère de l'Intérieur sera fournie au Titulaire par l'Acheteur lors du démarrage des prestations.

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

Dans le cas où des écarts sont identifiés, le Titulaire propose les corrections à apporter et les soumet à l'Acheteur pour validation. L'Acheteur est le seul à pouvoir approuver une mise à jour du PAS.

Le Titulaire doit décrire dans le PAS l'ensemble des indicateurs SSI qu'il juge utile au suivi de la sécurité en phase projet et opérationnelle. Le Titulaire doit fournir mensuellement à l'Acheteur, une mise à jour de ces indicateurs.

Le Titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournies à l'Acheteur et précisé dans le PAS. Dans ce cadre, le Titulaire notifie à l'Acheteur toute information permettant d'améliorer le niveau de sécurité du système d'information et signaler les difficultés et risques que certains choix peuvent entraîner.

Dans l'hypothèse où le Titulaire ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le marché pour s'exonérer de ses obligations contractuelles.

4.2 Hébergement des données et des services

Le Titulaire doit mettre en place des mécanismes/outils de protection pour lutter contre :

- Les attaques classiques sur IP et les protocoles associés (Par exemple : Attaque de type déni de service).
- Les codes malveillants pouvant affecter la disponibilité, compromettre la sécurité ou consommer de manière excessive les ressources de l'application. Ces mécanismes/outils doivent être détaillés dans le PAS.

L'accès aux systèmes de l'Acheteur par des personnels d'exploitation doit se faire par authentification forte. Dans le cas contraire, le Titulaire doit indiquer dans le PAS les mesures mises en place pour assurer la légitimité des accès ainsi que l'imputabilité et la traçabilité des actions de ses personnels.

Le Titulaire doit mettre en place les mesures et dispositions adéquates pour assurer la continuité des services rendus par les systèmes de l'Acheteur dont il est responsable dans le cadre de la prestation. Les mesures permettant la continuité des services sont définies en adéquation avec le besoin identifié en disponibilité.

L'ensemble de ces mesures et dispositions doit être détaillé dans le plan de continuité d'activité (PCA) du Titulaire. Le Titulaire doit garantir la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information dans les délais convenus dans le plan de continuité d'activité.

4.1 Conseil et de conformité à l'état de l'art

Le Titulaire garantit à l'Acheteur qu'il est conforme à l'état de l'art pour les services et objets numériques fournis dans le cadre des prestations. Sur demande de l'Acheteur, le Titulaire fournit la preuve de cette conformité sous 7 jours ouvrables. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (*appareils connectés, sauvegardes de données, consoles d'administration*).

Le Titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournies à l'Acheteur. Dans ce cadre, le titulaire notifie à l'acheteur toute information permettant d'améliorer le niveau de sécurité du système d'information et signaler les difficultés et risques que certains choix peuvent entraîner. Dans l'hypothèse où le Titulaire ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le marché pour s'exonérer de ses obligations contractuelles.

Le Titulaire met en œuvre les pratiques de sécurité et emploie des outils qui soient adaptés aux enjeux de sécurité de l'Acheteur, et proportionnés à la menace pouvant s'exercer sur les biens à protéger. Il détaille dans le PAS les outils qu'il utilise dans le cadre des prestations du marché.

4.3 Cartographie des systèmes d'information

Le Titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il a la charge et doit les maintenir, selon les préconisations de l'ANSSI issues du guide « Cartographie des systèmes d'information ».

Le modèle de cartographie du Titulaire doit obligatoirement faire l'objet d'une validation par le responsable sécurité de l'Acheteur.

L'inventaire et la cartographie sont livrés sous 7 jours ouvrables à la demande de l'Acheteur et au minimum une fois par semestre.

4.4 Protection de l'information

Le Titulaire s'engage à mettre en œuvre les mesures adéquates permettant de garantir la protection des informations sensibles de l'Acheteur. Le Titulaire s'engage ainsi à appliquer le plan de classification, règle de marquage et de traitement de données définis dans le corpus de la sécurité numérique du ministère de l'Intérieur ou à préciser dans le PAS, la correspondance vis-à-vis de sa propre classification.

Les données de l'Acheteur, quel que soit leur support, sont strictement couvertes par le secret professionnel (article 226-13 du code pénal).

Le Titulaire s'engage à prendre toutes les précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le Titulaire s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel :

- Ne prendre aucune copie des documents et supports d'informations confiés, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation envers l'Acheteur ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées dans les prestations couvertes par le marché remporté par le Titulaire ;

- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- Prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la durée du présent contrat.

Il est rappelé qu'en cas de non-respect des dispositions précitées, la responsabilité du Titulaire peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du code pénal.

Le Titulaire a l'obligation de mettre en place un inventaire identifiant tous les documents de l'Acheteur en sa possession, quel que soit leur classification et leur version. Sur demande de l'Acheteur, le Titulaire communique cet inventaire sous 7 jours ouvrés à partir de la date de la demande.

Le Titulaire ne pourra pas sous-traiter l'exécution des prestations à une autre société qui n'assurerait pas un niveau de sécurité similaire à celui du Titulaire, ni procéder à une cession de marché.

Le Titulaire met à disposition de l'Acheteur, sur demande et dans un délai de sept (7) jours ouvrés à partir de la date de demande de l'Acheteur, l'ensemble de ses documents relatifs aux politiques et procédures de sécurité, applicables dans le cadre des prestations du marché.

4.5 Maintien en condition de sécurité

Au titre du MCS, le Titulaire s'assure en permanence que le système reste apte à remplir sa mission de protection de l'information, à compter de l'installation sur site des premiers composants et tout au long de la vie du système.

Le Titulaire doit n'utiliser que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée du marché. Si la durée du marché dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le Titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus.

Une vérification d'aptitude (VA) ou vérification d'aptitude au bon fonctionnement (VABF) ou une vérification de service régulier (VSR) peuvent être refusées si des composants ne sont pas à jour des correctifs de failles de sécurité publiés depuis un délai supérieur aux seuils prévus dans le présent document.

Le Titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances du système ou sa compatibilité aux éléments employés par l'Acheteur pour l'utilisation du système (ex : navigateur Firefox, etc.), en modifiant si besoin et à ses frais le système, pour maintenir le niveau de performance et la conformité à la matrice de compatibilité, malgré l'application du correctif.

Le Titulaire ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations qu'il fournit à l'emploi de composants dans une version non supportée, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de réduire les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi. Dans tous les cas le maintien en condition opérationnelle (MCO), la tierce maintenance applicative (TMA) ou simplement l'hébergement incluent le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité.

4.6 Information sur les événements et incidents de sécurité

Nom du livrable	Délai de livraison
Fiches réflexes (FR)	T0 + 3 mois et en tant que de besoin en cas d'évolution du système ou lors du processus de capitalisation sur les événements rencontrés

Pour les prestations, produits et services fournis par le Titulaire dans le cadre du marché, celui-ci met à disposition un canal d'information dédié à la sécurité informatique (liste de diffusion par courriel ou autre) permettant de tenir l'Acheteur informé des événements et incidents de sécurité, notamment liés à la connaissance d'une vulnérabilité impactant le système (annonce de correctif, attaque en cours, violation de données à caractère personnel si le traitement de données est sous-traité au Titulaire), et des mesures correctives ou conservatoires à appliquer.

Le Titulaire réalise des fiches réflexes en vue de prévoir les actions et décisions à prendre suite à un incident. Le Titulaire veille à mettre à jour ces fiches réflexes en fonction des incidents qu'il serait amené à gérer durant toute la durée du marché.

4.7 Sécurité des locaux du Titulaire

Dans le cas où des informations sensibles, quel que soit leur marquage et quelle que soit la forme de leur support, sont appelées à être conservées dans les locaux du titulaire, leur support papier ou électronique doivent être disposés en dehors de leur utilisation dans des armoires fermant à clé et dont la clé est conservée par la seule personne responsable de leur utilisation.

A tout moment pendant l'exécution du marché, l'Acheteur se réserve le droit de réaliser tout contrôle, après un préavis de trois jours ouvrés, dans les locaux du Titulaire pour vérifier que sont effectivement respectées les préconisations validées par l'Acheteur s'agissant des règles de gestion et des mesures techniques de sécurisation des moyens de traitement des informations sensibles du ministère.

En cas de défaillance constatée dans la mise en œuvre de mesures de sécurité en adéquation avec le niveau de sensibilité des données traitées, il pourra être fait obligation au Titulaire de réaliser à ses frais tous travaux de mise en conformité de ses locaux.

Le Titulaire a le devoir d'informer sans délai l'Acheteur de toute difficulté dans l'application de ces mesures, de fuite ou de suspicion de fuite d'informations sensibles qu'il rencontre ou constate.

4.8 Echéance ou résiliation du marché

Au terme du marché ou en cas de résiliation, le titulaire restitue sans délai à l'acheteur une copie de l'intégralité des données qui lui ont été confiées (*directement par l'acheteur ou produit par le titulaire pour le compte de l'Acheteur*) dans le cadre de la prestation.

Un procès-verbal de restitution doit être établi par le Titulaire qui identifie le représentant de l'Acheteur à qui sont remis les données sur support électronique et la liste des données remises.

Une fois la restitution du procès-verbal effectuée, le Titulaire doit détruire, dans un délai de trois (3) mois maximum après la fin du marché, les éventuelles données détenues dans son système d'information, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage.

Le Titulaire établit alors un procès-verbal de destruction qui doit systématiquement préciser la liste des données remises, certifier avoir détruit toutes les données listées ainsi que toute copie éventuelle et indiquer les moyens de destruction utilisés.

En fonction du marquage apposé sur les documents, le Titulaire veille à respecter les procédés de destruction conformément aux réglementations en vigueur.

A la fin de la prestation, le titulaire doit restituer les matériels fournis par l'Acheteur (cartes à puce, postes de travail, ...).

4.9 Audit de sécurité sur le périmètre du Titulaire

L'Acheteur peut réaliser, ou faire réaliser à ses frais par un organisme qu'il mandate à cette fin, un audit de sécurité sur le périmètre du Titulaire ou, le cas échéant, de ses sous-traitants, afin de s'assurer de l'application effective des exigences de sécurité imposées par l'Acheteur. Le Titulaire est informé 15 jours à l'avance (date de l'audit, modalités financières pour l'Acheteur et le prestataire pressenti pour réaliser l'audit, ...).

L'Acheteur, ou l'organisme qu'il mandate à cette fin, peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du Titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées. Le Titulaire est informé quinze 15 jours à l'avance (date de l'audit, modalités

Le Titulaire effectue des autocontrôles de conformité aux exigences du marché pour garantir et maintenir un niveau de sécurité adéquat durant toute la durée de la prestation. Ceux-ci doivent à minima être réalisés annuellement.

Le Titulaire doit être en mesure d'apporter la preuve de ces autocontrôles sur demande de l'Acheteur.

En cas de constatation d'écarts aux exigences de sécurité imposées par l'Acheteur, un plan de remédiation devra être formalisé par le Titulaire 15 jours ouvrables après la constatation des écarts.

Le Titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties ou, pour le cas des correctifs techniques, conformément aux délais de maintien de condition de sécurité fixés dans le CCTP. Sur la base de ces contrôles effectués, le Titulaire doit rendre compte des résultats à l'Acheteur à l'occasion de comités de sécurité. Les retards peuvent donner lieu à des pénalités financières, et le cas échéant, être une cause de rupture de contrat.

L'Acheteur peut réaliser ou faire réaliser à ses frais, par un organisme mandaté à cette fin ou une solution automatisée, des audits techniques permettant de rechercher, détecter et évaluer la robustesse des développements, outils, mécanismes ou configurations mis en œuvre sur le périmètre du Titulaire ou ses sous-traitants dans le cadre du marché. Le délai de préavis de l'Acheteur pour mener ces audits est de 15 jours ouvrés maximum.

5. EXIGENCES TECHNIQUES APPLICABLES AUX SYSTEMES D'INFORMATION

5.1 Processus d'homologation des SI

Tout système d'information traitant des informations ou supports à protéger doit faire l'objet d'une homologation, consistant en la déclaration par une autorité dite d'homologation, que le système d'information considéré est apte à traiter des informations ou supports protégés conformément aux objectifs de sécurité visés, et qu'elle accepte les risques de sécurité résiduels induits.

La démarche d'homologation de sécurité suit le cycle de vie de la cible. C'est pourquoi tout au long du marché les éléments constitutifs du dossier de sécurité seront amenés à évoluer dans la limite de ce qui est prévu par la réglementation et les directives associées.

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

1.1.1 Exigence SECU HOM 001

Dans ses travaux d'ingénierie, le Titulaire doit proposer des solutions techniques qui ne constituent pas un obstacle au prononcé de l'homologation du système d'information.

1.1.2 Exigence SECU HOM 002

Le Titulaire fournira les éléments nécessaires à l'établissement et au maintien à jour des documents du dossier en vue du maintien de l'homologation des systèmes de l'Acheteur.

1.1.3 Exigence SECU HOM 003

Le Titulaire doit rédiger et maintenir à jour l'analyse de risques du système en vue d'identifier les risques auxquels l'application est confrontée.

Cette action doit identifier les principaux risques pesant sur les valeurs métiers fournies par l'application, ainsi que les mesures à mettre en œuvre pour diminuer la vraisemblance des scénarios de risque.

1.1.4 Exigence SECU HOM 004

Le Titulaire réalise et met à jour les dossiers d'architecture de l'ensemble des systèmes d'information de l'Acheteur. Ces documents doivent être marqués « Diffusion Restreinte » et traitent systématiquement des sujets suivants :

- Détail de l'architecture fonctionnelle : description des échanges métiers permettant au système de remplir sa mission ;
- Détail de l'architecture applicative : description des différentes briques applicatives du système, des échanges entre ces dernières et des fonctionnalités métiers associées ;
- Détail de l'architecture technique : description du socle technique sur lequel s'appuie le projet et les flux techniques associés (serveurs, stockage, réseau, sauvegarde) ;
- Détail de la résilience du système : capacité à continuer de rendre le service en cas de défaillance d'un composant technique ;
- Gestion des journaux d'évènements ;
- Description des mesures de sécurité permettant de garantir la confidentialité, l'intégrité et la disponibilité du système (durcissement des serveurs, identification/authentification, haute disponibilité, ...).

1.1.5 Exigence SECU HOM 005

Le Titulaire doit justifier dans le DAT les mécanismes de sécurité mis en place dans la solution en vue de répondre aux objectifs de sécurité identifiés dans l'analyse de risque. Ces objectifs peuvent être satisfaits par un logiciel personnalisé, un logiciel tiers ou l'environnement technique de la solution.

1.1.6 Exigence SECU HOM 006

Le Titulaire réalise la PES regroupant à minima les points suivants :

- Organisation de la sécurité ;
- Sécurité physique ;
- Sécurité des personnes ;
- Sécurité des documents ;
- Sécurité du système d'information ;
- Résilience du système d'information.

Note : L'Acheteur peut mettre à disposition du Titulaire (ou l'annexer directement au marché) le modèle de PES proposé dans la DISSIP en précisant néanmoins que le Titulaire doit éviter les redondances entre ce document et le PAS.

1.1.7 Exigence SECU HOM 008

Le Titulaire doit faire réaliser des audits de sécurité (Test d'intrusion, architecture, configuration et audit de code) tous les deux ans. Le rapport d'audit doit obligatoirement être communiqué au CSN de l'Acheteur qui est systématiquement invité à la réunion de lancement et de restitution.

Le Titulaire doit lancer les premiers audits dans les six mois suivant la notification du marché ou avant la mise en production du système. Le délai de deux ans court à partir de la livraison du premier rapport d'audit.

Note :

- *La liste des audits à faire réaliser par le Titulaire peut être modifiée en fonction des besoins de l'acheteur. Pour les systèmes ouverts sur Internet, les tests d'intrusion ont un caractère obligatoire conformément à la DISSIP.*
- *Pour les systèmes d'information les plus sensibles, il convient de faire réaliser les audits par des prestataires qualifiés PASSI par l'ANSSI.*

1.1.8 Exigence SECU HOM 009

Le Titulaire tient à jour les analyses de risque afin de prendre en compte les vulnérabilités résiduelles et conceptuelles. Il élabore des scénarios d'attaques puis en chiffre les impacts sur le système d'information de l'Acheteur.

Le Titulaire justifie dans ce document, le cas échéant, qu'une vulnérabilité identifiée ne peut pas être exploitée dans l'environnement prévu pour le produit.

1.1.9 Exigence SECU HOM 010

Lorsqu'une vulnérabilité affectant l'un des systèmes d'information de l'Acheteur, ne peut pas être corrigée ou contournée, le Titulaire met à jour l'analyse de risques du système et la transmet au plus tôt au CSN de l'Acheteur.

1.1.10 Exigence SECU HOM 011

Tout document du dossier d'homologation doit être expressément validé par le CSN de l'Acheteur afin d'être considéré comme finalisé. La validation est considérée comme tacite au-delà d'une période de soixante (60) jours à partir de la date de livraison au CSN de l'Acheteur.

5.2 Maintenance en condition de sécurité

Au titre du MCS, le Titulaire s'assure en permanence que le système reste apte à remplir ses missions conformément aux enjeux de sécurité identifiés, à compter de l'installation sur site des premiers composants et tout au long de la vie du système.

5.1.1 Exigence SECU MCS 001

Le Titulaire fournit les solutions de lutte contre les codes malveillants utilisés sur les systèmes des différents projets de l'Acheteur ainsi que les mises à jour de sécurité de l'ensemble des constituants des systèmes selon une fréquence et des procédures qui sont définies et acceptées par l'Acheteur.

Note : Cette exigence n'est pas applicable aux SI hébergés dans les data centers du ministère de l'Intérieur, pour lesquels les solutions antivirales sont fournies par l'Administration.

5.1.2 Exigence SECU MCS 002

Le Titulaire met en œuvre une veille de sécurité pour l'ensemble des produits (logiciels et matériels) de l'Acheteur, relevant du marché. Cette veille permet d'identifier les vulnérabilités relatives à ces produits et les correctifs de sécurité disponibles. La veille de sécurité au titre du

MCS doit être réalisée en utilisant plusieurs sources distinctes (éditeurs, sites institutionnels...), incluant le CERT-FR.

5.1.3 [Exigence SECU MCS 003](#)

En cas de mise en évidence d'une vulnérabilité affectant un système de l'Acheteur relevant du marché, le Titulaire collabore avec l'Acheteur pour déterminer l'origine de la vulnérabilité et les actions à engager pour sa résolution.

Cette activité consiste à :

- Maintenir une veille sur les produits et collecter, agréger et synthétiser les informations traitant des évolutions de la menace et des vulnérabilités ;
- Collecter les alertes (bulletins) de sécurité observés en production ;
- Analyser la criticité d'une alerte ou d'un incident sur le système concerné ;
- Proposer des solutions de contournement en cas d'urgence (impossibilité de déployer rapidement un correctif) ;
- Recevoir/Récupérer un correctif ;
- Qualifier le correctif ;
- Déployer le correctif ;
- Entretenir la documentation système.

5.1.4 [Exigence SECU MCS 004](#)

L'évaluation de la criticité doit utiliser la méthode CVSS (Common Vulnerability Scoring System). Le système CVSS propose le calcul de trois notes comprises entre 0 (risque nul) et 10 (risque très élevé) :

- Note de base : impact maximum théorique ;
- Note temporelle : note de base pondérée par les correctifs existants ou à contrario les « exploits » ;
- Note environnementale : note temporelle affinée selon les déploiements des systèmes et leur contexte opérationnel. Cette note doit être soumise par le Titulaire au responsable sécurité de l'Acheteur (ou un représentant habilité par l'Acheteur) pour validation ou modification.

L'échelle de criticité de la version 3.1 du système CVSS doit être utilisée par le Titulaire lors de sa requalification de la note CVSS des vulnérabilités émises par les différentes sources du Titulaire (ex : CERT-FR).

5.1.5 [Exigence SECU MCS 005](#)

Les vulnérabilités découvertes au titre du MCS sont traduites sous forme de fiches de fait technique de sécurité (FTS) permettant d'en assurer le suivi. Leur traitement (contournement ou correction) est réalisé dans un délai correspondant à un niveau de risque (criticité) décidé en partenariat avec l'Acheteur.

5.1.6 [Exigence SECU MCS 006](#)

Pour les vulnérabilités de criticité « Nul » ou « Faible » découvertes au titre du MCS, le Titulaire applique un correctif suite à sa découverte d'une faille :

- Dans les douze (12) mois pour les failles dont la note CVSS est égale à 0.
- Dans les six (6) mois pour les failles dont la note CVSS est comprise entre 0 et 3,9.

Les délais sont comptés à partir de la validation par l'Acheteur de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

5.1.7 [Exigence SECU MCS 007](#)

Pour les vulnérabilités de criticité « Moyen » découvertes au titre du MCS, le Titulaire :

- Applique, si cela est techniquement possible, une mesure de contournement dans le mois ;
- Trouve et applique un correctif dans les trois (3) mois pour les failles dont la note CVSS est comprise entre 4 et 6,9.

Les délais sont comptés à partir de la validation par l'Acheteur de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

5.1.8 [Exigence SECU MCS 008](#)

Pour les vulnérabilités de criticité « Elevé » découvertes au titre du MCS, le Titulaire :

- Applique une mesure de contournement dans les sept (7) jours ;
- Trouve un correctif dans le mois pour les failles dont la note CVSS est comprise entre 7 et 8,9. En fonction des contraintes techniques, l'application du correctif peut être décalée en commun accord avec l'Acheteur et sur justification dûment motivée par le Titulaire.

Les délais sont comptés à partir de la validation par l'Acheteur de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

5.1.9 [Exigence SECU MCS 009](#)

Pour les vulnérabilités de criticité « Critique » découvertes au titre du MCS, le Titulaire :

- Applique, si cela est techniquement possible, une mesure de contournement dans les quarante-huit (48) heures ;
- Trouve et applique un correctif dans les sept (7) jours pour les failles dont la note CVSS est supérieure ou égale à 9. En fonction des contraintes techniques, l'application du correctif peut être décalée en commun accord avec l'Acheteur et sur justification dûment motivée par le Titulaire.

Les délais sont comptés à partir de la validation par l'Acheteur de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

5.1.10 [Exigence SECU MCS 010](#)

Le Titulaire assure le MCS dès la conception ou les évolutions des différents systèmes de l'Acheteur.

5.1.11 [Exigence SECU MCS 011](#)

Le Titulaire analyse pour toute modification d'un des systèmes de l'Acheteur réalisée au titre du MCS, les impacts sur la sécurité du système. Cette analyse doit être détaillée dans le document d'analyse de risque du projet, en précisant notamment :

- La description détaillée des modifications ;
- Les éventuelles vulnérabilités engendrées par les modifications ;
- L'impact de ces vulnérabilités sur le système ;
- Les solutions mises en place pour diminuer le risque associé aux modifications (action sur les vulnérabilités ou sur les impacts) ;
- Une estimation du risque résiduel après mise en place des solutions de diminution du risque.

5.1.12 [Exigence SECU MCS 012](#)

Le Titulaire fournit et réalise des tests de non régression relatifs à la sécurité puis respecte le passage en comité de changement conformément aux procédures de l'Acheteur. Les différents scénarii de tests sont détaillés dans le PMCS.

5.1.13 [Exigence SECU MCS 013](#)

Le Titulaire garantit que le canal d'approvisionnement des correctifs de sécurité est de confiance.

Le Titulaire garantit l'origine, assure un contrôle d'intégrité et en garde une trace pouvant être un élément de preuve en cas d'audit (par exemple : Procès-Verbal de livraison signé).

5.1.14 Exigence SECU MCS 014

Le Titulaire offre les moyens d'appliquer les correctifs de sécurité sur chaque composant (système ou applicatif) des systèmes de l'Acheteur. Cette mise à jour du système est la plus automatisée possible et est tracée dans les journaux.

5.1.15 Exigence SECU MCS 015

Le Titulaire effectue la mise à jour des documents du dossier de sécurité impactés par les mises à jour du système. A fortiori, le Titulaire met à jour l'analyse de risques du système en cas d'impossibilité de correction d'une vulnérabilité identifiée.

5.1.16 Exigence SECU MCS 016

Le Titulaire identifie, au titre du MCS, les versions de logiciels obsolètes ou qui vont le devenir. Un logiciel qui n'est plus soutenu au niveau sécurité est déclaré obsolète. Cette déclaration est anticipée par le Titulaire en contactant les éditeurs pour obtenir leur calendrier de soutien (calendriers publiés pour les systèmes d'exploitation grand public par exemple).

5.1.17 Exigence SECU MCS 017

Le Titulaire met en place une gestion de configuration permettant d'assurer l'intégrité et l'authenticité des composants ou correctifs livrés et leur déploiement sur les plates-formes.

5.1.18 Exigence SECU MCS 018

Le Titulaire garantit que toute évolution majeure des systèmes de l'Acheteur s'appuie sur des versions de logiciels à jour en terme de correctifs et annoncées maintenues pendant au moins la durée de MCO contractualisée.

5.3 Etat de l'art

5.3.1 Exigence SECU EDA 001

Le Titulaire conçoit, met en œuvre et exploite les systèmes d'information sous sa responsabilité conformément à l'état de l'art en matière de sécurité numérique. 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, le Titulaire doit respecter les exigences suivantes pour les services Web et de messagerie qu'il serait amené à fournir :

- **Services Web :**
 - les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, ...) ou une technologie en particulier ;
 - les mécanismes cryptographiques doivent être conformes aux annexes B du référentiel général de sécurité (RGS)1 de l'ANSSI.
 - 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 ;
 - 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 ;
 - 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 ;
 - 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 messagerie :**

- les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, ...) ;
- la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (norme SPF), signature numérique (norme DKIM), politique de sécurité liant le tout (norme DMARC)).

Dans le cas où l'une des exigences ne peut être appliquée, le Titulaire le fait savoir au plus tôt à l'Acheteur. Le Titulaire veille à exercer son devoir de conseil en proposant des mesures permettant de garantir, si cela est possible, un niveau de sécurité identique aux exigences supra dont seul l'Acheteur peut valider ou non l'application.

5.4 Gestion des biens de l'Acheteur

5.4.1 Exigence SECU_GDB_001

Le Titulaire conserve et traite les données de l'Acheteur 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'Acheteur suivant le principe de restriction au besoin d'en connaître. L'Acheteur doit donner ses performances dans le CCTP : droits d'accès, machines virtuelles séparées, disques séparés, machines physiques séparées.

5.4.2 Exigence SECU_GDB_002

Le Titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.

5.4.3 Exigence SECU_GDB_003

Le Titulaire garantit que les supports échangés ou à connecter sur un SI de l'Acheteur 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'Acheteur.

5.4.4 Exigence SECU_GDB_004

Toute transmission de fichiers sur un support physique (DAT, CDROM, ...), 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'Acheteur. 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 :

- L'émetteur et le destinataire ;

<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/>

- Le détail des opérations de transferts et notamment le nombre, la date. Sur simple demande, ce registre est mis à la disposition de l'Acheteur adjudicateur par le Titulaire.

5.4.5 Exigence SECU_GDB_005

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.

5.4.6 Exigence SECU_GDB_006

Le Titulaire conserve en lieu sûr les supports de stockage en fin de vie hébergeant des données de l'Acheteur, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée résiduelle ne puisse être récupérée. En cas d'impossibilité de réaliser un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne ou dysfonctionnement), le disque dur ou la mémoire doit être détruit(e) physiquement avant de quitter définitivement le service ou démonté(e) et entreposé(e) dans un local sécurisé en attente de destruction.

5.4.7 Exigence SECU GDB 007

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'Acheteur.

5.4.8 Exigence SECU GDB 008

Le Titulaire maintient à jour et est en mesure de mettre à disposition de l'Acheteur toutes les données relatives à la prestation.

5.4.9 Exigence SECU GDB 009

Il est fait obligation au Titulaire que le traitement des informations sensibles sur support électronique ne soit pas réalisé sur des moyens informatiques connectés à un réseau non maîtrisé. L'Acheteur considère qu'un réseau d'entreprise connecté à Internet ne permet pas de garantir ce niveau adéquat de protection des informations sensibles.

Le cas échéant, le Titulaire peut s'efforcer de démontrer à l'Acheteur son aptitude à protéger les informations sensibles qu'il serait amené à traiter en dehors des systèmes d'information de l'Acheteur.

Pour ce faire :

- Soit l'isolation des moyens de traitement des informations s'effectue de manière physique ;
- Soit cette isolation s'effectue par une interface logique de sécurité présentant des garanties suffisantes afin d'empêcher l'accès aux moyens de traitement des informations sensibles par des tiers.

Le Titulaire doit alors détailler dans le PAS les règles de gestion et les règles techniques de sécurité de ces moyens de traitement des informations sensibles. Ces règles de gestion et règles techniques de fonctionnement concourant à la sécurité des informations sensibles doivent faire l'objet d'une validation formelle par l'Acheteur. Ce dernier se réserve le droit de procéder à leur contrôle préalablement à toute validation comme après validation pendant l'exécution du marché.

5.5 Sécurité de ses locaux informatiques

5.5.1 Exigence SECU LOC 001

En cas de changement de localisation des données ou services, le Titulaire en informe préalablement l'Acheteur.

5.5.2 Exigence SECU LOC 002

A la première demande de l'Acheteur, 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.

5.5.3 Exigence SECU LOC 003

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.

5.5.4 Exigence SECU LOC 004

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'Acheteur et équipements de sûreté.

5.5.5 Exigence SECU LOC 005

Les locaux du Titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, ...) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- 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.

5.5.6 Exigence SECU LOC 006

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, ...) sont accompagnées par une personne habilitée.

5.5.7 Exigence SECU LOC 007

En cas de mutualisation de ses plateaux, le Titulaire met en place les mesures pour protéger les espaces attribués à l'Acheteur pour la prestation effectuée (accès aux baies par carte, espace privatif grillagé, ...).

5.5.8 Exigence SECU LOC 008

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'Acheteur 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'Acheteur de celles des autres clients au sein des salles informatiques :

- la salle hébergeant des matériels de l'Acheteur doit si possible lui être dédiée ;
- Dans le cas où la séparation physique des salles n'est pas possible, le Titulaire fournit à l'Acheteur 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.

5.5.9 [Exigence SECU LOC 009](#)

Le Titulaire assure la protection de la documentation de l'Acheteur 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.

5.6 Sécurité des réseaux et de l'exploitation

5.6.1 [Exigence SECU SRE 001](#)

Le Titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

5.6.2 [Exigence SECU SRE 002](#)

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 permettant l'accès aux environnements de l'Acheteur depuis le site du Titulaire doivent respecter les exigences suivantes (en suivant, à défaut d'une précision de l'Acheteur, les recommandations de l'ANSSI) :

- Les correctifs de sécurité et les mises à jour antivirus doivent se faire quotidiennement ;
- Tous les outils présents sur le poste doivent être référencés dans le CCT du ministère de l'Intérieur. Toute dérogation doit être expressément validée par le CSN de l'Acheteur ;

Les postes ne doivent pas avoir accès à internet et à un système d'information bureautique (messagerie, intranet, ...) ;

Les postes d'administration utilisés doivent être réservés exclusivement à cet usage. Tout accès au poste doit se faire de manière sécurisée que ce soit pour l'ouverture d'une session et l'accès physique ;

Les postes d'administration doivent être mis sur un VLAN dédié.

Si un tel dispositif s'avère impossible à réaliser pour le Titulaire, l'Acheteur peut mettre à disposition, aux frais du Titulaire, des postes portables sécurisés pour les activités d'exploitation et de TMA.

5.6.3 [Exigence SECU SRE 003](#)

L'installation, l'exploitation et l'administration des produits mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'Acheteur. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'Acheteur.

A ce titre, les mots de passe hérités des paramétrage d'usine des produits doivent systématiquement être modifiés lors de leur configuration pour les besoins de l'Acheteur.

5.6.4 [Exigence SECU SRE 004](#)

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 validée par l'Acheteur.

5.6.5 [Exigence SECU SRE 005](#)

Le Titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'Acheteur.

5.6.6 [Exigence SECU SRE 007](#)

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.

5.6.7 Exigence SECU SRE 008

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'Acheteur) dispose d'un compte individuel qui peut être :

- 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 ;
- Soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en étant toujours attribué qu'à une seule personne à la fois.

5.6.8 Exigence SECU SRE 009

Le Titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. Il précise dans le PAS, la procédure de revue de ces comptes. Le cas échéant, il automatise le processus de blocage ou de suppression.

5.6.9 Exigence SECU SRE 010

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.

5.6.10 Exigence SECU SRE 011

Le Titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'Acheteur existants ainsi que des rôles et privilèges qui y sont associés. Il fournit cette liste à l'Acheteur sur demande. Le Titulaire effectue et formalise une revue trimestrielle des comptes d'accès aux serveurs et autres ressources du Titulaire utilisées dans le cadre de la prestation.

5.6.11 Exigence SECU SRE 012

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 et erreur sur les secrets d'authentification.

5.6.12 Exigence SECU SRE 013

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 :

- Connexion et déconnexion aux équipements et applications ;
- Consultations d'informations relatives à la vie privée ;
- Informations d'usage de l'Internet (accès aux sites Web) ;
- Accès en lecture et/ou en écriture à des fichiers et dossiers identifiés comme sensibles ;
- 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.

5.6.13 Exigence SECU SRE 015

Le Titulaire respecte la politique de définition des mots de passe de l'Acheteur sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du Titulaire.

5.6.14 Exigence SECU SRE 016

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'Acheteur.

5.6.15 Exigence SECU SRE 017

Le Titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'Acheteur dans le cadre de la prestation.

5.6.16 Exigence SECU SRE 018

Le Titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et aux traitements des incidents, pour la tenue de ses engagements contractuels.

5.6.17 Exigence SECU SRE 019

Le Titulaire est capable de fournir à l'Acheteur, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI de l'Acheteur en astreinte.

5.6.18 Exigence SECU SRE 020

Le Titulaire est responsable de l'analyse des traces systèmes, applicatives et réseaux en vue de détecter toute attaque ou tentative d'attaque et, le cas échéant, ajuster les configurations et paramètres de sécurité.

Toute attaque fait l'objet d'une fiche d'alerte à l'équipe SSI de l'Acheteur précisant a minima :

- Un résumé de l'attaque (en précisant son vecteur) et ses impacts potentiels ;
- L'adresse IP de l'attaquant ;
- Les impacts de l'attaque sur l'écosystème du système d'information cible (avec une note CVSS) ;
- Les actions à mettre en œuvre (Contournement ou correctif) ;
- La date de correction envisagée.

Les délais de correction sont assujettis à la note CVSS de la fiche d'alerte et doivent respecter les mêmes contraintes temporelles que celles indiquées dans le cadre du MCS.

5.7 Sécurité de ses postes de travail

5.7.1 Exigence SECU SPT 001

En vue de prévenir le vol des données de l'Acheteur contenues dans les postes de travail nomade du Titulaire, celui-ci met systématiquement en place les mesures de protection suivantes :

- Câbles antivols et filtre de confidentialité ;
- Installation d'une solution de chiffrement surfacique nécessitant de préférence une authentification forte pour le déchiffrement.

5.7.2 Exigence SECU SPT 002

Le Titulaire applique une durée de verrouillage automatique de session sur l'ensemble des postes qu'il met à disposition de ses personnels. Cette durée ne doit pas excéder l'heure.

5.7.3 Exigence SECU SPT 003

Le Titulaire doit privilégier l'authentification forte pour tout déverrouillage de session des postes de travail bureautique.

5.7.4 Exigence SECU SPT 004

Le Titulaire rend obligatoire l'utilisation de l'authentification forte (ex. carte à puce, token usb, ...) au poste de travail utilisé pour l'administration technique des systèmes de l'Acheteur.

5.7.5 Exigence SECU SPT 005

Tous les postes de travail du Titulaire doivent disposer d'une solution de chiffrement robuste, qualifiée par l'ANSSI afin de permettre le chiffrement des données sensibles de l'Acheteur que les personnels du Titulaire seraient amenés à stocker ou communiquer dans le cadre de leurs missions.

5.8 Traitement des incidents de sécurité

5.8.1 Exigence SECU INC 001

Le service de supervision du Titulaire met en place un système de remontée d'alerte à l'Acheteur, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations sensibles appartenant à l'Acheteur (documentations technique en particulier).

5.8.2 Exigence SECU INC 002

Le Titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

5.8.3 Exigence SECU INC 003

Le Titulaire contacte les interlocuteurs sécurité de l'Acheteur désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'Acheteur :

- Si cet incident a lieu sur le SI de l'Acheteur, le Titulaire participera à la demande de l'Acheteur au traitement de l'incident ;
- Si cet incident a lieu sur le SI du Titulaire, le Titulaire autorisera l'Acheteur ou un tiers désigné à participer au traitement de l'incident (si l'Acheteur le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'Acheteur (traitement des causes profondes).

5.8.4 Exigence SECU INC 004

Le Titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit à l'Acheteur sur demande.

5.8.5 Exigence SECU INC 005

Le Titulaire prévoit dans sa procédure de gestion des incidents un chapitre sur la conservation et la consultation des traces utiles pour mener une analyse forensique suite à une suspicion d'attaque ou une analyse post incident.

5.9 Accès aux locaux de l'Acheteur

5.9.1 Exigence SECU AL 001

Tout personnel du Titulaire, que celui-ci soit l'un de ses salariés ou salarié d'un des sous-traitants du Titulaire, devant avoir accès aux locaux de l'Acheteur doit être nommément agréé selon la procédure en vigueur dans les locaux de l'Acheteur.

Le personnel du Titulaire est soumis pendant son séjour aux mêmes règles intérieures que les agents de l'Acheteur, notamment les politiques et procédures de sécurité des systèmes d'information, ainsi que les chartes administrateurs et utilisateurs. L'Acheteur peut retirer son agrément à tout moment sans avoir à énoncer ses motifs, le Titulaire devra proposer un remplaçant conformément aux exigences mentionnées supra.

5.9.2 Exigence SECU AL 002

L'intervention dans les data centers du ministère de l'Intérieur est conditionnée à l'obtention d'une autorisation d'accès délivrée au personnel du Titulaire après enquête diligentée par le service de sécurité compétent pour l'autorité contractante au profit de laquelle le marché est exécuté. Le délai d'enquête est en moyenne de quinze (15) jours ouvrés et il est fait obligation au Titulaire de fournir à l'Acheteur :

- Le patronyme et les prénoms de son agent ;
- Une photocopie lisible et recto-verso d'un titre d'identité dont la nature varie selon la situation individuelle de l'agent visé :
 - o une carte nationale d'identité (CNI) ou un passeport, en cours de validité, pour les ressortissants français et communautaires ;
 - o pour les systèmes d'information qui ne sont pas soumis à la mention de protection « Spécial France » : un titre de séjour en cours de validité avec une autorisation de travail valable ou carte de résident pour les étrangers extracommunautaires ;
 - o un justificatif de domicile de moins de trois (3) mois si l'adresse de l'agent diffère de celle portée sur le titre d'identité fourni.

5.10 Intervention au sein des locaux de l'Acheteur

5.10.1 Exigence SECU TIERS 001

Au même titre que les agents de l'Acheteur, le Titulaire doit prendre connaissance et appliquer les référentiels internes de l'Acheteur (politiques de sécurité numérique, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, ...).

5.10.2 Exigence SECU TIERS 002

Le Titulaire ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

5.10.3 Exigence SECU TIERS 003

Le Titulaire ne doit connecter au réseau interne de l'Acheteur que des équipements fournis par ce dernier. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, ...).

5.10.4 Exigence SECU TIERS 004

Le Titulaire élabore et maintient un inventaire complet et à jour des matériels mis à sa disposition par l'Acheteur. Cette liste doit être transmise semestriellement au responsable désigné par l'Acheteur.

5.10.5 Exigence SECU TIERS 005

Le Titulaire tient à jour la liste exhaustive des comptes d'accès aux systèmes d'information de l'Acheteur existants ainsi que des rôles et privilèges qui y sont associés. Il doit être en mesure de fournir cette liste à l'Acheteur sur demande. Le Titulaire doit également effectuer et formaliser une revue semestrielle des comptes d'accès aux serveurs et autres ressources de l'Acheteur utilisées par le Titulaire dans le cadre du marché.

5.11 Nomadisme numérique

Dans le cadre de certaines prestations, quand cela est autorisé par l'Acheteur, il peut être envisagé que le Titulaire puisse se connecter à distance aux SI de l'Acheteur, notamment durant les périodes d'astreinte.

5.11.1 Exigence SECU NOMADE 001

Dans le cas où l'Acheteur autorise formellement les accès distants vers ses systèmes d'information, le Titulaire met en place les solutions permettant de sécuriser ces accès distants et d'enregistrer les activités des intervenants pour les nécessités d'investigation, notamment en cas de crise cyber.

5.11.2 Exigence SECU NOMADE 002

Le Titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex : VPN IPSec) pour la connexion à distance aux réseaux utilisés dans le cadre de la Prestation (que ce soient ceux du Titulaire, ceux de l'Acheteur ou les deux éventuellement). Le personnel du Titulaire devra explicitement lancer la connexion et s'authentifier pour obtenir l'accès à distance aux SI de

l'Acheteur (connexion authentifiée non permanente) ou utiliser les services et moyens d'accès distants mis à disposition par l'Acheteur.

5.11.3 Exigence SECU NOMADE 003

Le Titulaire restreint la connexion distante des personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion distante non autorisée en horaires ouvrées), et aux ressources nécessaires en astreinte uniquement.

5.12 *Interconnexion avec les SI du Titulaire*

Dans le cadre de certaines prestations, une interconnexion est réalisée entre les SI de l'Acheteur et du Titulaire. Cette interconnexion doit être cadrée avec vigilance et respecter se conformer aux politiques, procédures et doctrines du ministère de l'Intérieur.

5.12.1 Exigence SECU INTERCO 001

Au même titre que les agents de l'Acheteur, le Titulaire prend connaissance et applique les règlements internes de l'Acheteur (Politiques et directives de sécurité, ...).

5.12.2 Exigence SECU INTERCO 002

Le Titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation. Il doit remonter au plus tôt à l'Acheteur toute anomalie lui permettant d'accéder de manière privilégiée à des ressources qui ne relèvent pas de sa responsabilité.

5.12.3 Exigence SECU INTERCO 003

En cas d'interconnexion des SI de l'Acheteur 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'Acheteur au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'Acheteur.

5.12.4 Exigence SECU INTERCO 004

Pour chaque interconnexion, les éléments suivants doivent être précisés dans la cartographie :

- 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...

5.13 *Prestations d'Etude*

Les prestations d'études nécessitent l'intégration de certaines clauses spécifiques. Elles représentent ici toutes les prestations faisant intervenir des Titulaires en phase projet (des phases d'étude des besoins aux phases de test en passant par les phases de conception), sans action de développement.

5.13.1 Exigence SECU CPE 001

Le Titulaire doit respecter les standards et les méthodologies préconisés au sein de l'Acheteur. 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.

5.13.2 Exigence SECU CPE 002

Le Titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de préproduction.

5.13.3 Exigence SECU CPE 003

Lors de la conduite de tests de validation ou du déploiement, le Titulaire doit :

- Utiliser des données de tests anonymisées (sauf accord formel de l'Acheteur) ;
- Ne pas provoquer de perturbations du système d'information de l'Acheteur lors des séances de test ;
- Remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible.

5.14 **Sécurité des développements**

5.14.1 Exigence SECU DEV 001

Le Titulaire doit prioriser les logiciels du cadre de cohérence technique de l'Acheteur ou du catalogue de l'ANSSI.

5.14.2 Exigence SECU DEV 002

Le Titulaire doit indiquer dans le PAS, la méthodologie adoptée pour assurer un développement sécurisé et d'audit des applications web (Par exemple, en s'appuyant sur les guides mis à disposition par l'OWASP ou la norme ISO 27034 relative à la sécurité applicative). Toute méthodologie doit a minima prendre en compte les points suivants :

- **Validation et codage.** Les exigences doivent préciser les règles pour canoniser, valider et coder chaque entrée à l'application, que ce soit des utilisateurs, des systèmes de fichiers, des bases de données, des répertoires ou des systèmes externes. La règle par défaut doit être que toutes les entrées sont invalides, à moins qu'elles ne correspondent à une spécification détaillée de ce qui est permis.

De plus, les exigences doivent préciser l'action à prendre, lorsqu'une entrée invalide est reçue. Précisément, l'application ne doit pas être susceptible aux injections, aux débordements, aux violations, ou d'autres attaques d'entrée corrompue. En conséquence, les réponses aux exigences suivantes doivent apparaître clairement dans le PAS :

- Les entrées des utilisateurs doivent être contrôlées et filtrées (longueur, type de donnée attendue, ...) avant traitement.
- Les contrôles de sécurité sur les entrées et les sorties d'une application doivent être réalisés à minima du côté du composant serveur de l'application.
- Seules les données correspondant à des paramètres attendus doivent être prises en compte.
- Toute donnée reçue par le composant serveur d'une application doit être expurgée des éléments pouvant être mal interprétés ou exécutés, avant transmission à une ressource utilisatrice (navigateur internet, moteur de base de données, moteur applicatif, ...).
- **Authentification et gestion de session :** Les exigences doivent préciser comment les authentifiants et les identifiants de session seront protégés à travers leur cycle de vie. Les exigences pour toutes les fonctions reliées, y compris les mots de passe oubliés, les mots de passe changeants, le rappel des mots de passe, la déconnexion et les connexions multiples doivent être incluses.
- **Contrôle d'accès :** Les exigences doivent inclure une description détaillée de tous les rôles (groupes, privilèges, autorisations) utilisés dans l'application. Les exigences doivent également inclure tous les biens et fonctions fournis par l'application. Les exigences doivent complètement préciser les droits d'accès exacts de chaque bien et fonction pour chaque rôle. Une matrice de contrôle d'accès est le format suggéré pour ces règles.

- **Gestion d'erreur** : Les exigences doivent détailler la façon dont les erreurs survenant pendant le traitement seront gérées. Certaines applications devraient fournir des résultats selon le meilleur effort, dans l'éventualité d'une erreur, tandis que d'autres devraient mettre fin au traitement immédiatement. Il **convient** que tout message d'erreur technique présenté à l'utilisateur soit personnalisé de façon à ne pas divulguer d'information sur les composants techniques sous-jacents.
- **Journalisation** : Les exigences doivent préciser que les événements portant sur la sécurité doivent être journalisés, comme les attaques détectées, les tentatives échouées d'ouverture de session, et les tentatives de dépasser les autorisations. Les exigences doivent également préciser l'information à saisir avec chaque événement, y compris l'heure et la date, la description de l'événement, les détails de l'application et autre information utile dans les efforts d'investigation informatique. Toute anomalie ou non-conformité identifiée par un contrôle de sécurité doit faire l'objet d'une trace.
- **Connexions aux systèmes externes** : Les exigences doivent préciser comment l'authentification et le chiffrement seront gérés pour tous les systèmes externes, comme les bases de données, les répertoires et les services Web. Tous les authentifiants nécessaires pour la communication avec les systèmes externes seront stockés à l'extérieur du code dans un fichier de configuration, sous forme chiffrée.
- **Contrôle des fichiers transmis** : Lorsqu'une application permet le téléchargement montant (upload) ou descendant (download) de fichiers, un contrôle strict doit être effectué sur chaque fichier reçu ou émis. Ce contrôle doit porter à minima sur le type, la taille et la localisation sur le système de fichiers.
- **Chiffrement** : Les exigences devront préciser quelles données doivent être chiffrées, comment elles doivent être chiffrées et comment tous les certificats et autres authentifiants doivent être gérés. L'application devra utiliser un algorithme standard implanté dans une bibliothèque de chiffrement largement utilisée et testée.
- **Disponibilité** : Les exigences doivent préciser comment elles protégeront contre les attaques de refus de service. Toutes les attaques possibles sur l'application devraient être considérées, y compris le verrouillage de l'authentification, l'épuisement de la connexion et d'autres attaques d'épuisement des ressources.
- **Configuration sécurisée** : Les exigences doivent préciser que les valeurs par défaut pour toutes les options de configuration pertinentes de sécurité doivent être sécurisées. Aux fins de vérification, le logiciel devrait pouvoir produire un rapport facilement lisible, montrant tous les détails pertinents de configuration de sécurité.
- **Vulnérabilités spécifiques** : Les exigences devront inclure un ensemble de vulnérabilités précises qui ne doivent pas être retrouvées dans le logiciel. Si non autrement spécifié, alors le logiciel ne doit inclure aucune des défaillances décrites dans la liste « OWASP Top Ten Most Critical Web Application Vulnerabilities. » (Dix plus cruciales vulnérabilités d'application Web de l'OWASP).

5.14.3 Exigence SECU_DEV_003

Le Titulaire doit fournir et suivre un ensemble de lignes directrices de codage de sécurité et d'utiliser un ensemble d'interfaces communes de programmation de contrôle de la sécurité (comme l'OWASP ESAPI). Ces lignes directrices doivent indiquer comment le code sera formaté, structuré et commenté.

Les interfaces communes de programmation de contrôle de la sécurité doivent définir comment les contrôles de sécurité doivent être nommés et comment les contrôles de sécurité doivent fonctionner.

Tout le code portant sur la sécurité doit être soigneusement commenté. Une orientation précise sur l'évitement des vulnérabilités de sécurité sera incluse.

Tout le code doit également être révisé au moins par un autre développeur, selon les exigences de sécurité et les lignes directrices de codage, avant qu'il ne soit considéré comme étant prêt pour les modules d'essai.

Le Titulaire veille à ce que le code source soit nettoyé des éléments de test et de débogage avant toute livraison à l'Acheteur.

5.14.4 Exigence SECU DEV 004

Le Titulaire doit être en capacité d'apporter les éléments de preuve permettant de certifier que le logiciel satisfait aux exigences de sécurité, que toutes les activités de sécurité ont été effectuées et que tous les problèmes de sécurité identifiés ont été documentés et résolus.

5.14.5 Exigence SECU DEV 005

Le Titulaire doit rédiger des spécifications de sécurité et vérifier les fonctions de sécurité conformément aux exigences de vérification d'une norme convenue (comme OWASP ASVS). Le Titulaire documentera les constatations de vérification, conformément aux exigences de rapport de la norme. Sur demande de l'Acheteur, le Titulaire doit pouvoir lui fournir les constatations de vérification sous sept (7) jours ouvrés.

5.14.6 Exigence e SECU DEV 006

Le Titulaire doit détailler dans la PES du système, les configurations et mécanismes de sécurité mis en place sur les logiciels et matériels livrés à l'Acheteur.

5.14.7 Exigence SECU DEV 007

La sécurité de toutes les applications développées par le Titulaire doit être systématiquement validée par des audits de sécurité visant à identifier les vulnérabilités potentielles (revue de code, tests des mécanismes de sécurité, ...).

5.14.8 Exigence SECU DEV 008

Les développements effectués sous la responsabilité du Titulaire font partie du périmètre de l'activité de veille sécurité au titre du MCS.

A ce titre, le Titulaire doit mettre en place les processus et/ou outils permettant de garantir qu'aucun composant présentant des vulnérabilités connues pouvant mettre en péril la sécurité des systèmes d'information de l'Acheteur, ne soient accidentellement inclus dans la solution au cours des développements.

5.14.9 Exigence SECU DEV 009

Le Titulaire doit utiliser un système de contrôle du code source qui authentifie les personnels contributeurs et journalise tous les modifications au produit de base du logiciel.

5.14.10 Exigence SECU DEV 010

Le Titulaire doit garantir que les environnements de développement, de qualification, de pré production et de production seront séparés de manière logique et/ou physique.

5.14.11 Exigence e SECU DEV 011

Le Titulaire est responsable de l'émission des certificats électroniques pour ses propres plateformes (développement, intégration, ...). L'Acheteur fournira uniquement les certificats pour ses propres plateformes (qualification, préproduction et production).

5.14.12 Exigence SECU DEV 012

Les données utilisées dans la constitution de jeux d'essais sur toutes les plateformes hors production ne doivent pas comporter de données réelles. Si des données réelles sont utilisées pour alimenter des plateformes différentes de celles de production, le Titulaire utilisera un outil permettant d'anonymiser les données. Le Titulaire précisera dans le PAS la méthode d'anonymisation choisie.

5.14.13 Exigence SECU DEV 013

Le Titulaire doit sauvegarder et conserver chaque version du code source ayant fait l'objet d'une phase de recette par l'Acheteur. Sur demande de l'Acheteur, le Titulaire doit être en capacité de fournir une copie de la sauvegarde sous quinze (15) jours ouvrés à partir de la date de demande.

5.14.14 Exigence SECU DEV 014

Le Titulaire doit procéder à la livraison des codes sources des différentes versions des livrables conformément aux exigences applicables au niveau de sensibilité dudit code conformément aux règles de sécurité numérique du ministère de l'Intérieur sur le traitement de l'information.

5.14.15 Exigence SECU DEV 015

Lors de la conduite de tests de validation ou du déploiement, le Titulaire doit :

- Utiliser des données de tests anonymisées ;
- Ne pas provoquer de perturbations du système d'information de l'Acheteur lors des séances de tests ;
- Être en capacité de remettre en l'état initial les systèmes testés ;
- Ne pas introduire de régression vis-à-vis d'un état de sécurité atteint dans une version précédente.

5.14.16 Exigence SECU DEV 016

L'Acheteur se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le Titulaire, via des audits et/ou des tests d'intrusion par exemple (audit de code sur les parties les plus sensibles, ...).

En cas de mise en évidence d'un manque de qualité avéré (hétérogénéité des mécanismes, ...) ou de sécurité (non-respect des standards cryptographiques, ...), la correction du code de l'application est au frais du Titulaire.

5.15 Achats de services, matériels ou logiciels

5.15.1 Exigence SECU AML 001

Le Titulaire s'engage à ce que les produits du contrat soient, au jour de leur mise en production, dépourvus de toute faille, faiblesse ou défaut de conception connues pouvant porter atteinte, directement ou indirectement à la sécurité des informations de l'Acheteur.

5.15.2 Exigence SECU AML 002

Dans le cadre d'une opération de maintenance, le Titulaire s'engage à chiffrer ou effacer de manière sécurisée toutes les données avant l'envoi en maintenance externe de toute ressource informatique de l'Acheteur.

Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance externe ne peut se faire que sous couvert d'un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un membre de l'équipe locale chargée des systèmes d'information.

Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l'envoi en maintenance externe est interdit.

5.15.3 Exigence SECU AML 003

Dans le cadre d'un accès à distance à une ressource informatique (matériel, logiciel) de l'Acheteur, le Titulaire doit présenter des mesures de sécurité renforcées validées par l'Acheteur.

Exemples de mesures de sécurité renforcées :

- Sécurisation de l'infrastructure de raccordement réseau ;
- Mise en place de mots de passe spécifiques pour l'accès en télémaintenance, respectant des règles de robustesse et de renouvellement ;
- Activation sur demande des accès entrant en télémaintenance. Par défaut, les accès entrants doivent être inactifs ;
- Journalisation des accès en télémaintenance ;
- Interdiction des possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local de l'Acheteur et plus largement vers les réseaux interurbains (WAN) nationaux.
- Pour toute mise au rebut définitive d'un matériel ou logiciel du service, le Titulaire doit empêcher de manière sécurisée l'accès aux données présentes sur les disques durs ou dans la mémoire intégrée.

Un procès-verbal doit être signé entre le Titulaire et l'Acheteur.

5.15.4 Exigence SECU AML 004

Le Titulaire veille à privilégier les solutions logicielles ou matérielles labélisées (qualifiées ou certifiées) par l'ANSSI sur les systèmes d'information qu'il serait amenés, dans le cadre du marché, à mettre en œuvre pour ses propres besoins ou concevoir pour les besoins de l'Acheteur. Si le produit final vise une qualification après la notification du marché, il est fortement recommandé que le jalon J0 du processus de qualification soit franchi préalablement.

Dans le cas où aucune solution du catalogue de l'ANSSI ne pourrait répondre au besoin de l'Acheteur, le Titulaire en formalise systématiquement les raisons et reste force de proposition et de conseil pour garantir la sécurité des informations de l'Acheteur durant toute la durée du marché.

Sur demande de l'Acheteur, le Titulaire doit fournir sous sept (7) jours ouvrés, les attestations de qualification ou de certification des solutions utilisées.

5.15.5 Exigence SECU AML 005

Pour les services d'hébergement externalisés à destination des systèmes de l'Acheteur, le Titulaire doit utiliser des services localisés sur le territoire national conformément à la PSSI de l'État.

NB : Afin d'ouvrir le champ des possibles, il peut être exigé du Titulaire de veiller à ce que l'hébergeur n'expose pas les systèmes de l'Acheteur à des fuites de données en les exposants à l'application de lois extraterritoriales (FISAA, Cloud Act, ...).

5.16 Gestion des droits d'accès

5.16.1 Exigence SECU ACCES 001

Le Titulaire doit mettre en place sur l'ensemble du parc de serveurs de l'Acheteur, des comptes d'accès nominatifs. Les droits des personnels d'exploitation doivent être limités au strict nécessaire pour la bonne réalisation de leurs missions. Les différents profils et les droits associés sont détaillés dans la PES.

5.16.2 CCTP-Exigence SECU ACCES 002

Le Titulaire doit veiller à limiter les droits des accès d'une application aux seuls fichiers dont elle est légitime d'accéder.

Le Titulaire décrit dans la PES les règles de durcissements mises en œuvre pour s'assurer du respect de cette exigence, dès la phase de conception d'une application ou lors de son intégration sur les serveurs de l'Acheteur.

5.16.3 Exigence SECU ACCES 003

Le Titulaire doit garantir que l'accès d'une application à une base de données se fait avec un compte spécifique bénéficiant des privilèges nécessaires et strictement suffisants.

5.16.4 Exigence SECU ACCES 004

Le Titulaire doit privilégier les plateformes SSO (Single Sign-On) de l'Acheteur pour toute application qu'il serait amené à développer ou paramétrer pour le compte de l'Acheteur et dont les besoins en confidentialité et/ou de traçabilité sont très forts. Dans le cas d'un hébergement externalisé, le Titulaire veille à proposer des solutions d'authentification adaptées aux enjeux du système d'information.

5.17 *Gestion des personnels*

5.17.1 Exigence SECU PERS 001

Le Titulaire est responsable de vérifier que tous les membres de l'équipe de développement ont été formés dans les techniques sécurisées de programmation. A ce titre, le Titulaire précise dans le PAS la manière dont il veille à employer des personnels qualifiés dans le cadre des prestations rendues à l'Acheteur.

5.17.2 Exigence SECU PERS 002

Le Titulaire effectue les enquêtes sur le casier judiciaire (demande du bulletin n°3) de tous les personnels du Titulaire amenés à intervenir dans le cadre du marché. Aucun personnel ne doit intervenir sur le périmètre de l'Acheteur sans une vérification préalable de ses antécédents judiciaires.

Le Titulaire doit être en mesure d'apporter la preuve de la gestion de ces opérations de contrôles. Un personnel présentant des antécédents judiciaires incompatibles avec les enjeux des activités de l'Acheteur, est récusé par défaut.

5.17.3 Exigence SECU PERS 003

Le Titulaire a obligation de communiquer mensuellement au responsable désigné par l'Acheteur, la liste de ses agents, que ceux-ci soient salariés du Titulaire ou salariés d'un de ses sous-traitants susceptibles d'intervenir dans l'exécution du marché.

Tout changement dans la composition de cette liste doit être porté, sans délai, à la connaissance du responsable désigné par l'Acheteur. A défaut, un état des lieux annuel de cette liste doit être adressé à l'Acheteur à chaque date d'anniversaire de la signature du marché.

5.17.4 Exigence SECU PERS 004

Les opérations de maintenance sous la responsabilité du Titulaire sont exécutées par des personnels et sociétés habilités, sous la surveillance des personnels autorisés.

5.18 *Continuité d'activité*

5.18.1 Exigence SECU PCA 001

Pour chaque système d'information dont il a la charge dans le cadre du marché, le Titulaire élabore le bilan d'impact sur l'activité des systèmes d'information qu'il fait valider par l'Acheteur.

A partir de ce document, le Titulaire met en œuvre les dispositifs techniques permettant de garantir la disponibilité de l'ensemble des services liés à la prestation tout au long du marché (redondance des composants, système de sauvegarde, ...) et fournit, à la demande de l'Acheteur, la PES amendée avec ces éléments.

5.18.2 Exigence SECU PCA 002

Le Titulaire précise dans la PES, toutes les dispositions prises (matériels de secours, contrats de service, ...) pour remplacer rapidement tout matériel sous sa responsabilité, endommagé ou perdu (poste de travail, serveur, équipement réseau), qui est utilisé dans le cadre des prestations du marché.

5.18.3 Exigence SECU PCA 003

Le Titulaire effectue au moins annuellement des tests de restauration des sauvegardes effectuées sur les données des systèmes d'information de l'Acheteur qu'il héberge et/ou exploite selon les prestations du marché.

6. PROTECTION DES INFORMATIONS SENSIBLES

6.1 Principes

Toute information sensible du ministère de l'Intérieur doit être considérée comme un bien à protéger et ce tout au long de son cycle de vie.

Les niveaux de sensibilité des informations sont définis dans le tableau ci-après.

Niveau de sensibilité	Définition
Non sensible	Données ou informations pouvant être diffusées volontairement ou dont la diffusion involontaire à l'extérieur du ministère ne porte pas de préjudice pour lui, ses partenaires du service public ou privés.
Sensible	Données ou informations ne devant pas être rendues publiques et/ou restreintes à la diffusion d'un domaine spécifique.
Sensible « Diffusion Restreinte »	Données ou informations soumises à une restriction de diffusion particulière. La « diffusion restreinte » relève de la nécessité d'éviter la divulgation, dans le domaine public, d'informations dont le regroupement ou l'exploitation pourraient : <ul style="list-style-type: none">- conduire à la découverte d'une information classifiée ;- porter atteinte à la sécurité ou à l'ordre public, au renom des institutions, à la vie privée de leurs membres ;- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics.

Le titulaire s'engage à ce que les informations sensibles, pendant tout leur cycle de vie, ne puissent être portées, même fortuitement, à la connaissance de personnes n'ayant pas le besoin d'en connaître sauf accord préalable exprès et écrit de l'administration.

Dans les locaux du prestataire, les informations sensibles font l'objet d'une gestion spécifique.

Des informations sensibles peuvent se voir attribuer une protection par un marquage « Diffusion Restreinte » selon les règles posées par l'annexe 3 de l'IGI 1300. Les informations « Diffusion Restreinte » sont déterminées en fonction de la nature de la prestation et du type de données à protéger dans le marché.

Les informations sensibles considérées « Diffusion Restreinte » sont marquées avec la mention « Diffusion Restreinte » conformément au modèle ci-dessous :

DIFFUSION RESTREINTE

Pour les documents papier, cette mention « Diffusion Restreinte » est portée en haut de toutes les pages du document. Les informations techniques au format électronique, ne pouvant donc faire l'objet d'un marquage réglementaire comme indiqué ci-dessus (comme par exemple les journaux d'évènements, les fichiers de configuration, les Codes sources), sont de facto considérées comme « Diffusion Restreinte » et le titulaire a l'obligation d'appliquer les dispositions réglementaires qui s'imposent pour la gestion de ces données.

La réalisation d'une copie d'une information considérée « Diffusion Restreinte » sans autorisation préalable est considérée par l'administration comme une violation des dispositions relatives au respect du secret dans l'exécution du marché.

6.2 Protection des informations sensibles sur support papier

Le titulaire a l'obligation de mettre en place un système de gestion permettant d'identifier tous les documents comportant des informations sensibles, quel que soit leur marquage, et pour chacun de ces documents ainsi identifié :

- de connaître la liste des personnes physiques comme morales en ayant eu connaissance ou communication ;
- d'en connaître soit la date de restitution à l'administration soit la date de destruction, ainsi que le nom et la qualité de la personne ayant réalisé l'opération.

En cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie le ou les documents détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les agents du titulaire ayant assisté à la destruction en qualité de témoin(s), et le moyen de destruction utilisé (broyage ou incinération).

Ce bordereau est transmis, sans délai, à l'officier de sécurité du PSSI, à l'adresse suivante :

dnum-mpssi@interieur.gouv.fr

Le bordereau de destruction stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles.

En cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui est remis le document. Au surplus, le bordereau doit stipuler que le titulaire certifie n'avoir ni établi ni conservé de copie du document.

La diffusion des documents papier se fait sous double enveloppe. L'enveloppe extérieure ne porte aucune mention particulière hormis le nom et l'adresse du destinataire. L'enveloppe interne porte le nom du destinataire et la mention pertinente, à savoir « Sensible » ou « Diffusion Restreinte ». Les agents du titulaire qui gèrent les arrivées courrier doivent être sensibilisés à l'usage de ces mentions, ne pas ouvrir l'enveloppe et la distribuer au destinataire.

6.3 Protection des informations sensibles sur support électronique

Il est fait obligation au titulaire que le traitement des informations sensibles sur support électronique ne soit pas réalisé sur des moyens informatiques connectés à un réseau non maîtrisé. L'administration considère qu'un réseau d'entreprise connecté à Internet ne permet pas de garantir ce niveau adéquat de protection des informations sensibles.

Le cas échéant, le titulaire peut s'efforcer de démontrer à l'administration son aptitude à protéger les informations sensibles qu'il serait amené à traiter en dehors des systèmes d'information du ministère de l'Intérieur. Pour ce faire :

- soit l'isolation des moyens de traitement des informations s'effectue de manière physique ;
- soit cette isolation s'effectue par une interface logique de sécurité présentant des garanties suffisantes afin d'empêcher l'accès aux moyens de traitement des informations sensibles par des tiers.

Le titulaire doit alors soumettre à l'administration une documentation relative aux règles de gestion et aux règles techniques de sécurité de ces moyens de traitement des informations sensibles. Ces règles de gestion et règles techniques de fonctionnement concourant à la sécurité des informations sensibles doivent faire l'objet d'une validation formelle par l'administration. Cette dernière se réserve le droit de procéder à leur contrôle préalablement à toute validation comme après validation pendant l'exécution du marché.

Il est fait obligation au titulaire de respecter le besoin d'en connaître : seuls ses agents de la Liste ont accès aux informations nécessaires pour l'exécution du marché. Le respect de cette obligation par le titulaire doit être garanti par la mise en place et l'utilisation de mécanismes de sécurité (authentification individuelle, gestion des droits et traçabilité des accès).

La confidentialité des informations sensibles, quel que soit leur marquage, sur support électronique est réalisée au moyen d'un mécanisme de chiffrement reposant sur un logiciel « qualifié » par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Ces logiciels sont fournis par l'administration dès notification du marché. Un document relatif à l'utilisation de ces logiciels est remis au titulaire dès notification du marché, il doit faire l'objet d'une diffusion auprès de ses agents intervenant dans le cadre des prestations prévues.

A l'issue du marché, le titulaire procède soit à la restitution, soit à la destruction de l'ensemble des informations sensibles sur support électronique et des documents associés incluant les courriels :

- en cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui sont remis les informations sensibles sur support électronique, en déclare la liste et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles ;
- en cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie les supports électroniques détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les agents du titulaire ayant assisté à la destruction en qualité de témoin(s), le ou les moyens de destruction utilisés. Ce bordereau est transmis, sans délai, à l'officier de sécurité du pôle SSI (PSSI), à l'adresse suivante :

dnum-mpssi@interieur.gouv.fr

Le bordereau de destruction stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles. Le mécanisme de destruction utilisé doit reposer sur un outil « qualifié » par l'ANSSI. Le cas échéant, cet outil est fourni par l'administration.

6.4 Sécuration des locaux du titulaire

Dans le cas où des informations sensibles, quel que soit leur marquage et quelle que soit la forme de leur support, sont appelées à être conservées dans les locaux du titulaire, leur support papier ou électronique doivent être disposés en dehors de leur utilisation dans des

armoires fermant à clé et dont la clé est conservée par la seule personne responsable de leur utilisation.

Préalablement à toute exécution du marché, le titulaire doit désigner un responsable sécurité qui devient l'interlocuteur privilégié de l'administration pour tous les sujets de sécurité pendant l'exécution du marché.

Il appartient à ce responsable sécurité de sensibiliser les agents du titulaire susceptibles d'intervenir dans l'exécution du marché au strict respect des obligations du titulaire en matière de SSI et d'en présenter un bilan à l'occasion de la réunion du comité de suivi ou de toute instance équivalente prévus dans les documents du marché.