



Cahier des Clauses Techniques Particulières (CCTP)

**Relatif à la tierce Maintenance Applicative de
l'application**

FNAEG-NG

Annexe 9

Exigences processus d'homologation des SI

Table des matières

1.1.1.1	Exigence SECU_HOM_001.....	6
1.1.1.2	Exigence SECU_HOM_002.....	6
1.1.1.3	Exigence SECU_HOM_003.....	6
1.1.1.4	Exigence SECU_HOM_004.....	6
1.1.1.5	Exigence SECU_HOM_005.....	6
1.1.1.6	Exigence SECU_HOM_006.....	6
1.1.1.7	Exigence SECU_HOM_008.....	7
1.1.1.8	Exigence SECU_HOM_009.....	7
1.1.1.9	Exigence SECU_HOM_010.....	7
1.1.1.10	Exigence SECU_HOM_011.....	8
1.1.2	Obligations du Titulaire sur le maintien en condition de sécurité	8
1.1.2.1	Exigence SECU_MCS_001.....	8
1.1.2.2	Exigence SECU_MCS_002.....	8
1.1.2.3	Exigence SECU_MCS_003.....	8
1.1.2.4	Exigence SECU_MCS_004.....	9
1.1.2.5	Exigence SECU_MCS_005.....	9
1.1.2.6	Exigence SECU_MCS_006.....	9
1.1.2.7	Exigence SECU_MCS_007.....	9
1.1.2.8	Exigence SECU_MCS_008.....	9
1.1.2.9	Exigence SECU_MCS_009.....	10
1.1.2.10	Exigence SECU_MCS_010.....	10
1.1.2.11	Exigence SECU_MCS_011.....	10
1.1.2.12	Exigence SECU_MCS_012.....	10
1.1.2.13	Exigence SECU_MCS_013.....	11
1.1.2.14	Exigence SECU_MCS_014.....	11
1.1.2.15	Exigence SECU_MCS_015.....	11
1.1.2.16	Exigence SECU_MCS_016.....	11
1.1.2.17	Exigence SECU_MCS_017.....	11
1.1.2.18	Exigence SECU_MCS_018.....	11
1.1.3	Obligations du Titulaire à se conformer à l'État de l'art.....	11
1.1.3.1	Exigence SECU_EDA_001	11
1.1.4	Obligations du Titulaire sur la gestion des biens de l'Acheteur	12
1.1.4.1	Exigence SECU_GDB_001	12
1.1.4.2	Exigence SECU_GDB_002	13
1.1.4.3	Exigence SECU_GDB_003	13
1.1.4.4	Exigence SECU_GDB_004	13
1.1.4.5	Exigence SECU_GDB_005	13
1.1.4.6	Exigence SECU_GDB_006	13
1.1.4.7	Exigence SECU_GDB_007	13
1.1.4.8	Exigence SECU_GDB_008	14
1.1.4.9	Exigence SECU_GDB_009	14
1.1.5	Obligations du Titulaire sur la sécurité de ses locaux informatiques	14

1.1.5.1	Exigence SECU_LOC_001.....	14
1.1.5.2	Exigence SECU_LOC_002.....	15
1.1.5.3	Exigence SECU_LOC_003.....	15
1.1.5.4	Exigence SECU_LOC_004.....	15
1.1.5.5	Exigence SECU_LOC_005.....	15
1.1.5.6	Exigence SECU_LOC_006.....	15
1.1.5.7	Exigence SECU_LOC_007.....	16
1.1.5.8	Exigence SECU_LOC_008.....	16
1.1.5.9	Exigence SECU_LOC_009.....	16
1.1.6	Obligations du titulaire sur la sécurité des réseaux et de l'exploitation	16
1.1.6.1	Exigence SECU_SRE_001	16
1.1.6.2	Exigence SECU_SRE_002	16
1.1.6.3	Exigence SECU_SRE_003	17
1.1.6.4	Exigence SECU_SRE_004	17
1.1.6.5	Exigence SECU_SRE_005	17
1.1.6.6	Exigence SECU_SRE_007	17
1.1.6.7	Exigence SECU_SRE_008	18
1.1.6.8	Exigence SECU_SRE_009	18
1.1.6.9	Exigence SECU_SRE_010	18
1.1.6.10	Exigence SECU_SRE_011	18
1.1.6.11	Exigence SECU_SRE_012	18
1.1.6.12	Exigence SECU_SRE_013	18
1.1.6.13	Exigence SECU_SRE_015	19
1.1.6.14	Exigence SECU_SRE_016	19
1.1.6.15	Exigence SECU_SRE_017	19
1.1.6.16	Exigence SECU_SRE_018	19
1.1.6.17	Exigence SECU_SRE_019	19
1.1.6.18	Exigence SECU_SRE_020	19
1.1.7	Obligations du titulaire sur la sécurité de ses postes de travail	20
1.1.7.1	Exigence SECU_SPT_001	20
1.1.7.2	Exigence SECU_SPT_002	20
1.1.7.3	Exigence SECU_SPT_003	20
1.1.7.4	Exigence SECU_SPT_004	20
1.1.7.5	Exigence SECU_SPT_005	20
1.1.8	Obligations du titulaire sur le traitement des incidents de sécurité	20
1.1.8.1	Exigence SECU_INC_001	20
1.1.8.2	Exigence SECU_INC_002	21
1.1.8.3	Exigence SECU_INC_003	21
1.1.8.4	Exigence SECU_INC_004	21
1.1.8.5	Exigence SECU_INC_005	21
1.1.9	Obligations du Titulaire lors de l'accès aux locaux de l'Acheteur	21
1.1.9.1	Exigence SECU_AL_001	21
1.1.9.2	Exigence SECU_AL_002	22
1.1.10	Obligations du Titulaire intervenant au sein des locaux de l'Acheteur.....	22

1.1.10.1	Exigence SECU_TIERS_001	22
1.1.10.2	Exigence SECU_TIERS_002	23
1.1.10.3	Exigence SECU_TIERS_003	23
1.1.10.4	Exigence SECU_TIERS_004	23
1.1.10.5	Exigence SECU_TIERS_005	23
1.1.11	Obligations du Titulaire sur le nomadisme numérique	23
1.1.11.1	Exigence SECU_NOMADE_001	23
1.1.11.2	Exigence SECU_NOMADE_002	24
1.1.11.3	Exigence SECU_NOMADE_003	24
1.1.11.4	Obligations en cas d'interconnexion avec les SI du Titulaire	24
1.1.11.5	Exigence SECU_INTERCO_001	24
1.1.11.6	Exigence SECU_INTERCO_002	24
1.1.11.7	Exigence SECU_INTERCO_003	24
1.1.11.8	Exigence SECU_INTERCO_004	25
1.1.11.9	Obligations du Titulaire sur les prestations d'Etude	25
1.1.11.10	Exigence SECU_CPE_001	25
1.1.11.11	Exigence SECU_CPE_002	25
1.1.11.12	Exigence SECU_CPE_003	26
1.1.12	Obligations du Titulaire sur la sécurité des développements	26
1.1.12.1	Exigence SECU_DEV_001	26
1.1.12.2	Exigence SECU_DEV_002	26
1.1.12.3	Exigence SECU_DEV_003	28
1.1.12.4	Exigence SECU_DEV_004	28
1.1.12.5	Exigence SECU_DEV_005	28
1.1.12.6	Exigence SECU_DEV_006	28
1.1.12.7	Exigence SECU_DEV_007	28
1.1.12.8	Exigence SECU_DEV_008	29
1.1.12.9	Exigence SECU_DEV_009	29
1.1.12.10	Exigence SECU_DEV_010	29
1.1.12.11	Exigence SECU_DEV_011	29
1.1.12.12	Exigence SECU_DEV_012	29
1.1.12.13	Exigence SECU_DEV_013	30
1.1.12.14	Exigence SECU_DEV_014	30
1.1.12.15	Exigence SECU_DEV_015	30
1.1.12.16	Exigence SECU_DEV_016	30
1.1.13	Obligations du Titulaire sur les achats de services, matériels ou logiciels	30
1.1.13.1	Exigence SECU_AML_001	30
1.1.13.2	Exigence SECU_AML_002	31
1.1.13.3	Exigence SECU_AML_003	31
1.1.13.4	CCTP-Exigence SECU_AML_004	31
1.1.13.5	Exigence SECU_AML_005	32
1.1.14	Obligations du Titulaire dans la gestion des personnels	32
1.1.14.1	Exigence SECU_PERS_001	32
1.1.14.2	Exigence SECU_PERS_002	32

1.1.14.3 Exigence SECU_PERS_003 32

1.1.14.4 Exigence SECU_PERS_004 32

1.1.1.1 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.

1.1.1.2 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.

1.1.2 Obligations du Titulaire sur le maintien 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.

1.1.2.1 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.

1.1.2.2 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.

1.1.2.3 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).

1.1.2.4 Exigence SECU_MCS_005

Les vulnérabilités découvertes au titre du MCS sont traduites sous forme de fiche 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.

1.1.2.5 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.

1.1.2.6 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 livre 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.

1.1.2.7 Exigence SECU_MCS_008

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

- Applique, si cela est techniquement possible, 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.

1.1.2.8 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 livre 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.

1.1.2.9 Exigence SECU_MCS_010

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

1.1.2.10 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.

1.1.2.11 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.

1.1.2.12 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).

1.1.2.13 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.

1.1.2.14 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).

1.1.2.15 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.

1.1.2.16 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.

1.1.3 Obligations du Titulaire à se conformer à l'État de l'art

1.1.3.1 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.

1.1.4 Obligations du Titulaire sur la gestion des biens de l'Acheteur

1.1.4.1 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.

1.1.4.2 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.

1.1.4.3 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.

1.1.4.4 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 chez 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 ;
- 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.

1.1.4.5 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.

1.1.4.6 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.

1.1.4.7 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.

1.1.4.8 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.

1.1.4.9 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.

1.1.5 Obligations du Titulaire sur la sécurité de ses locaux informatiques

1.1.5.1 Exigence SECU_LOC_001

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

1.1.5.2 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.

1.1.5.3 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.

1.1.5.4 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.

1.1.5.5 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.

1.1.5.6 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.

1.1.5.7 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, ...).

1.1.5.8 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.

1.1.5.9 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.

1.1.6 Obligations du titulaire sur la sécurité des réseaux et de l'exploitation

1.1.6.1 Exigence SECU_SRE_001

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

1.1.6.2 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 paramétrages d'usine des produits doivent systématiquement être modifiés lors de leur configuration pour les besoins de l'Acheteur.

1.1.6.3 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.

1.1.6.4 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.

1.1.6.5 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.

1.1.6.6 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.

1.1.6.7 Exigence SECU_SRE_011

Le Titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'Acheteur existant 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.

1.1.6.8 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.

1.1.6.9 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.

1.1.6.10 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.

1.1.6.11 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.

1.1.7 Obligations du titulaire sur la sécurité de ses postes de travail

1.1.7.1 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.

1.1.7.2 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.

1.1.7.3 Exigence SECU_SPT_003

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

1.1.7.4 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.

1.1.7.5 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.

1.1.8 Obligations du Titulaire lors de l'accès aux locaux de l'Acheteur

1.1.8.1 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.

1.1.8.2 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 :
 - une carte nationale d'identité (CNI) ou un passeport, en cours de validité, pour les ressortissants français et communautaires ;
 - 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 ;
 - 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.

1.1.9 Obligations du Titulaire intervenant au sein des locaux de l'Acheteur

1.1.9.1 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, ...).

1.1.9.2 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.

1.1.9.3 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,...).

1.1.9.4 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.

1.1.9.5 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.

1.1.10 Obligations du Titulaire sur le 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.

1.1.10.1 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.

1.1.10.2 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 des prestations (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.

1.1.10.3 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.

1.1.10.4 Obligations du Titulaire sur les 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.

1.1.10.5 Exigence SECU_CPE_001

Le Titulaire doit respecter les standards et les méthodologies préconisés par 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.

1.1.10.6 Exigence SECU_CPE_003

Lors de la conduite des 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.

1.1.11 Obligations du Titulaire sur la sécurité des développements

1.1.11.1 Exigence SECU_DEV_001

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

1.1.11.2 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 à 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).

1.1.11.3 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.

1.1.11.4 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.

1.1.11.5 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.

1.1.11.6 Exigence 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.

1.1.11.7 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, ...).

1.1.11.8 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.

1.1.11.9 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.

1.1.11.10 Exigence SECU_DEV_010

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

1.1.11.11 Exigence 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).

1.1.11.12 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.

1.1.11.13 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.

1.1.11.14 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.

1.1.11.15 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.

1.1.11.16 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.

1.1.12 Obligations du Titulaire sur les achats de services, matériels ou logiciels

1.1.12.1 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.

1.1.12.2 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.

1.1.12.3 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.

1.1.12.4 CCTP-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 amené, 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 JO 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.

1.1.12.5 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, ...).

1.1.13 Obligations du titulaire sur la gestion des droits d'accès

1.1.13.1 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.

1.1.13.2 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.

1.1.13.3 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.

1.1.14 Obligations du Titulaire dans la gestion des personnels

1.1.14.1 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.

1.1.14.2 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 Judiciaire.

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.

1.1.14.3 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.

1.1.14.4 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.

