



MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉCONOMIE  
SÉCRÉTARIAT D'ÉTAT AU NUMÉRIQUE

Accord-cadre n°2024-0319

## ANNEXE 2 au Cahier des Clauses Techniques Particulières (CCTP)

Exigences de sécurité applicables aux  
différents lots \_ Spécifiques Programme  
France Identité Numérique  
Système de Gestion de l'Identité

## Table des matières

1	Exigences relatives au plan d'assurance sécurité.....	3
2	Exigences relatives à l'homologation des systèmes .....	3
3	Exigences relatives à la constitution du dossier de sécurité.....	4
4	Exigences spécifiques à la sécurité des développements.....	6
5	Exigences spécifiques au maintien en condition de sécurité.....	10
6	Exigences relatives aux droits d'accès.....	13
7	Exigences relatives aux personnels.....	14
8	Exigences relatives à l'hébergement et l'exploitation par un tiers .....	14
9	Annexe 1 : Exigences de sécurité globale.....	15
9.1	Clause de confidentialité .....	15
9.2	Clause de sécurité applicable à l'accès aux locaux.....	16
9.3	Protection des informations sensibles.....	16
9.3.1	Protection des informations sensibles sur support papier .....	17
9.3.2	Protection des informations sensibles sur support électronique .....	17
9.4	Clause relative à la restitution des informations.....	18
9.5	Clause relative à la sécurité des locaux du titulaire .....	18
10	Annexe 2 : Sanction pécuniaire pour non-respect des PSSI.....	<u>Erreur ! Signet non défini.</u> 18

## 1 EXIGENCES RELATIVES AU PLAN D'ASSURANCE SECURITE

### Exigence SECU\_PAS\_001

Le Titulaire doit rédiger le Plan d'Assurance Sécurité (PAS), précisant les engagements de ce dernier pour répondre aux exigences de sécurité de l'administration :

- Procédures de développements sécurisés des applicatifs (Cf. SECU\_DEV\_002) ;
- Procédures de sécurité liées à l'exploitation des SI de l'administration ;
- Habilitation des personnels ;
- Sécurité des locaux de développements ;
- Sécurité des locaux d'hébergement ;
- Sécurisation des livraisons ;
- Audit et revue des exigences de sécurité ;
- Etc.

Le PAS doit décrire l'organisation qui sera mise en place, la méthodologie appliquée pour gérer la sécurité des projets de l'administration et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre, notamment pour garantir les réponses aux exigences de sécurité du présent document.

### Exigence SECU\_PAS\_002

Le PAS doit reprendre, au minimum, l'ensemble des chapitres de la norme ISO 27002:2013. La mention « Sans Objet » devra être inscrite sous chaque partie non applicable.

### Exigence SECU\_PAS\_003

Le PAS doit se conformer aux exigences de sécurité détaillées dans les PSSI de l'administration durant toute la durée du marché.

## 2 EXIGENCES RELATIVES A L'HOMOLOGATION DES SYSTEMES

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.

### Exigence SECU\_HOM\_001

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

### Exigence SECU\_HOM\_002

Le Titulaire maintient à jour les éléments constitutifs du dossier de sécurité cités dans le présent document, afin de contribuer à l'acquisition et au maintien de l'homologation dans le temps des différents projets de l'administration.

### Exigence SECU\_HOM\_003

Le Titulaire se limite à la constitution des éléments requis par le dossier de sécurité. Ces éléments sont présentés à l'administration qui décide de les valider ou en demande au Titulaire la modification.

### **3 EXIGENCES RELATIVES A LA CONSTITUTION DU DOSSIER DE SECURITE**

Le Titulaire établit pour chaque projet, un dossier de sécurité 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.

Les documents constitutifs du dossier de sécurité spécifique à chaque projet, sont :

- Le rapport d'audit de sécurité du projet ;
- Le Dossier d'Architecture Technique (DAT) ;
- L'Analyse des Risques SSI du projet ;
- Le Dossier d'Analyse des Vulnérabilités Résiduelles (DAVR).
- Le dossier de sécurité comprend également les documents suivants, communs à l'ensemble des projets sous la responsabilité de l'administration :
  - La Procédure d'Exploitation de la Sécurité (PES) ;
  - Le Plan de Maintien en Condition de Sécurité (PMCS).

#### **Exigence SECU\_DOS\_001**

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'administration.

#### **Exigence SECU\_DOS\_002**

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 devrait identifier les principaux risques pesant sur les biens et fonctions essentiels fournis par l'application, ainsi que les mesures à mettre en œuvre pour diminuer la vraisemblance des risques.

#### **Exigence SECU\_DOS\_003**

Le Titulaire réalise ou met à jour les DAT de l'ensemble des systèmes de l'administration. Ces documents sont classifiés « Diffusion Restreinte » et traitent systématiquement des sujets suivants :

- Définition de l'architecture applicative : description des différentes briques applicatives du projet, des échanges entre ces dernières et des fonctionnalités métiers associées ;
- Définition de l'architecture logicielle ; description des composants logiciels constituant les briques applicatives du projet (serveur et poste de travail le cas échéant) ;
- Définition de l'architecture technique : description du socle technique sur lequel s'appuie le projet et les flux techniques associés ;
- Définition de la résilience du système : capacité à continuer de rendre le service en cas de défaillance d'un composant technique ;
- Dimensionnement (serveurs, stockage, réseau, sauvegarde) ;
- Description des mesures de sécurité en place (durcissement des serveurs, traçabilité, identification/authentification, etc.).

#### **Exigence SECU\_DOS\_004**

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 des risques. Ces objectifs peuvent être satisfaits par un logiciel personnalisé, un logiciel tiers ou l'environnement technique de la solution.

#### **Exigence SECU\_DOS\_005**

Le Titulaire réalise la PES regroupant au minimum les points suivants :

- Modalités d'installation, de paramétrage et de mise en œuvre de la sécurité ;
- Opérations d'administration, de gestion et de supervision de la sécurité ;
- Règles d'exploitation des composants du système ;
- Sauvegarde et restaurations ;
- Gestion des droits ;
- Emploi des moyens d'authentification ;
- Modalités de sensibilisation du personnel et des utilisateurs ;
- Chartes d'utilisation et d'administration ;
- Gestion des biens et des supports ;
- Enregistrement des incidents.

Une PES établie par l'administration sera mise à disposition du Titulaire afin qu'il puisse y apporter les compléments nécessaires.

#### **Exigence SECU\_DOS\_006**

Le Titulaire réalise des fiches réflexes en vue de prévoir les actions et décisions à prendre suite à un incident.

#### **Exigence SECU\_DOS\_007**

Le Titulaire constitue, pour chaque projet, les documents du dossier de sécurité spécifiques à ce dernier et les soumet à l'administration.

#### **Exigence SECU\_DOS\_008**

Le Titulaire décrit dans le PAS, les processus d'ingénierie de la SSI et la documentation associée.

#### **Exigence SECU\_DOS\_009**

Le Titulaire décrit dans ce processus d'ingénierie, les moyens qui concourent à assurer que les livrables produits respectent les exigences de sécurité.

#### **Exigence SECU\_DOS\_010**

Les Titulaires de lots qui implémentent des fonctions hébergées dans les infrastructures serveur du Ministère de l'Intérieur doivent faire réaliser des audits de sécurité (tests d'intrusion et audit de code) à la demande du programme et à minima tous les deux ans. Cet audit doit être réalisé par une société externe qualifiée PASSI par l'ANSSI. Le rapport d'audit doit obligatoirement être communiqué au RSSI de l'administration qui est systématiquement invité à la réunion de restitution.

#### **Exigence SECU\_DOS\_011**

Le Titulaire doit prévoir des clauses permettant à l'administration de réaliser des audits de conformité aux exigences de sécurité (Audit de conformité au PAS, etc.) ainsi que des audits de code sur les applications qui relèvent de leur périmètre de responsabilité. Le délai de préavis pour mener ces audits doit être de quinze (15) jours.

#### **Exigence SECU\_DOS\_014**

Le Titulaire réalise le Dossier d'Analyse des Vulnérabilités Résiduelles (DAVR) reprenant les vulnérabilités résiduelles et conceptuelles, élabore des scénarios d'attaques puis en chiffre les impacts sur le système d'information de l'administration.

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

#### **Exigence SECU\_DOS\_016**

Lorsqu'une vulnérabilité ne peut pas être corrigée et est acceptée par l'Autorité d'Homologation du projet concerné, le Titulaire met à jour le DAVR du système concerné.

#### **Exigence SECU\_DOS\_017**

Tout document du dossier de sécurité doit être expressément validée par le RSSI afin d'être considéré comme finalisé. Celle-ci peut être considérée comme tacite au-delà d'une période de 60 jours à partir de la date de livraison au RSSI de l'administration.

#### **Exigence SECU\_DOS\_018**

Le Titulaire précisera systématiquement dans le DAT les paramètres les plus pertinents à sélectionner ou à mettre en place au niveau des composants logiciels du projet pour sécuriser efficacement la plateforme.

#### **Exigence SECU\_DOS\_019**

Le Titulaire incorporera dans chaque analyse de risques un volet sur la sécurité des données à caractère personnel et l'impact sur la vie privée de la personne concernée, en cas de compromission ou altération de ces dernières.

## **4 EXIGENCES SPECIFIQUES A LA SECURITE DES DEVELOPPEMENTS**

#### **Exigence SECU\_DEV\_001**

Le Titulaire précise dans le PAS les outils et procédures qui seront utilisées pour garantir la sécurité au cours du développement.

Le PAS doit notamment inclure pour les services externalisés, les accords de confidentialité et de propriété intellectuelle protégeant les intérêts de l'administration, incluant également les sous-traitants travaillant à la maintenance des applicatifs.

#### **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, à partir des guides mis à disposition par l'OWASP). Toute méthodologie doit au minimum 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, etc.) avant traitement ;
  - Les contrôles de sécurité sur les entrées et les sorties d'une application doivent être réalisés au minimum 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, etc.).
- **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 et 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 'a-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).

#### **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 sera également 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 mise en production.

#### **Exigence SECU\_DEV\_004**

Le Titulaire doit 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. Toute livraison sans certification doit être justifiée expressément et documentée dans le détail dans le DAVR.

#### **Exigence SECU\_DEV\_005**

Le Titulaire doit rédiger des spécifications de sécurité et recetter les fonctions de sécurité (également appelée « vérification ») 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. Le Titulaire fournira les constatations de vérification à l'administration.

#### **Exigence SECU\_DEV\_006**

Le Titulaire convient de fournir des lignes directrices de configuration sécurisée qui décrivent entièrement les options pertinentes de configuration et leurs implications pour la sécurité globale du logiciel. Cette ligne directrice devra inclure une description complète des dépendances de la plateforme de support, y compris le système d'exploitation, le serveur Web et le serveur d'application, et la façon dont ils devraient être configurés pour la sécurité. La configuration par défaut du logiciel devra être sécurisée.

#### **Exigence SECU\_DEV\_007**

Le Titulaire doit mettre en place des guides et procédures de sécurité pour accompagner les différents acteurs qui interviendront dans la conception des systèmes et applications de l'administration.



**Exigence SECU\_DEV\_008**

Le Titulaire doit mettre en place des outils afin de s'assurer qu'aucun composant présentant des vulnérabilités critiques pour la sécurité, pouvant exposer les produits à des attaques connues, ne soient accidentellement inclus dans la solution au cours des développements.

**Exigence SECU\_DEV\_009**

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

**Exigence SECU\_DEV\_010**

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

**Exigence SECU\_DEV\_011**

Le Titulaire doit utiliser un système de contrôle du code source qui authentifie et journalise les membres d'équipe associés avec tous les changements au produit de base du logiciel et toute la configuration et tous les fichiers de conceptions reliés.

**Exigence SECU\_DEV\_012**

Le Titulaire doit préciser dans le DAT du système concerné, tout logiciel de tierce partie utilisé dans le logiciel, y compris toutes les bibliothèques, les cadres du travail, les composantes et autres produits, qu'ils soient commerciaux, libres, de source ouverte ou de source fermée.

**Exigence SECU\_DEV\_013**

Le Titulaire doit s'assurer que tous les composants logiciels externes utilisés satisfont à toutes les présentes exigences, et sont aussi sécurisés qu'un code personnalisé développé en vertu des présentes exigences.

**Exigence SECU\_DEV\_014**

Le Titulaire s'assure de maintenir l'architecture logicielle à l'état de l'art en termes de sécurité durant toute la durée de vie du marché. Les mises à jour doivent être effectuées à chaque nouvelle version livrée à l'administration.

**Exigence SECU\_DEV\_015**

Le Titulaire doit garantir la confidentialité de toutes les informations personnelles ou présentant un caractère sensible issues des environnements de production qui peuvent être utilisées dans la constitution de jeux d'essais. Le Titulaire précisera la méthode d'anonymisation choisie dans le PAS.

**Exigence SECU\_DEV\_016**

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

**Exigence SECU\_DEV\_017**

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

**Exigence SECU\_DEV\_018**

Les données utilisées dans le cadre de qualification (recettes) 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.

#### **Exigence SECU\_DEV\_019**

Le Titulaire devra être force de proposition et de conseil lors des développements des applications qui assureront un traitement sur des données à caractère personnel, pour respecter les exigences du Règlement Général de la Protection des Données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016).

## **5 EXIGENCES SPECIFIQUES AU MAINTIEN EN CONDITION DE SECURITE**

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.

#### **Exigence SECU\_MCS\_001**

Le Titulaire fournit les solutions de lutte contre les codes malveillants utilisés sur les systèmes des différents projets de l'administration 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'administration.

#### **Exigence SECU\_MCS\_002**

Le Titulaire met en œuvre une veille d'un point de vue de la sécurité pour l'ensemble des constituants matériels et logiciels des systèmes d'un projet de l'administration.

Cette veille permet d'identifier les vulnérabilités relatives à ces constituants et les correctifs de sécurité disponibles. La veille de sécurité au titre du MCS est réalisée, en utilisant plusieurs sources distinctes (éditeurs des constituants, sites institutionnels, etc.) incluant de préférence le CERT-FR.

Le Titulaire assure la couverture de l'ensemble des logiciels constituant les systèmes par les sources retenues (couverture à fournir).

#### **Exigence SECU\_MCS\_003**

Le Titulaire détecte les failles et les vulnérabilités sur les différents systèmes de l'administration et en suit leur 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 incidents de sécurité observés en production ;
- Analyser les impacts de la correction d'une alerte ou d'un incident sur le système concerné ;
- Proposer des solutions de contournement en cas d'urgence ;
- Recevoir un correctif ;
- Qualifier le correctif ;
- Déployer le correctif ;
- Entretenir la documentation système.

#### **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 RSSI l'administration ou l'autorité d'homologation pour validation ou modification.

L'échelle de criticité associée à la notation CVSS est la suivante :

- Nulle : note de 0 (sans objet) ;
- Faible : note de 0,1 à 2,9 inclus ;
- Moyenne : note de 3 à 6,9 inclus ;
- Forte : note de 7 à 8,9 inclus ;
- Maximale : note de 9 à 10 inclus.

#### **Exigence SECU\_MCS\_005**

Les vulnérabilités, anomalies ou bugs de criticité grave et majeure découverts au titre du MCS sont répertoriés sous forme de document de suivi des anomalies. Leur traitement (contournement ou correction) est réalisé dans un délai correspondant à un niveau de risque (criticité) décidé en partenariat avec l'administration. Ces délais sont précisés dans le CCTP.

#### **Exigence SECU\_MCS\_006**

Pour les vulnérabilités de criticité faible ou moyenne découvertes au titre du MCS, le Titulaire applique une mesure de contournement et applique un correctif en respectant les délais précisés dans le CCTP.

Les délais sont comptés à partir de la validation par l'administration de la note environnementale.

#### **Exigence SECU\_MCS\_007**

Pour les vulnérabilités de criticité grave découvertes au titre du MCS, le Titulaire applique une mesure de contournement et un correctif en respectant les délais précisés dans le CCTP.

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

#### **Exigence SECU\_MCS\_008**

- Pour les vulnérabilités de criticité majeure découvertes au titre du MCS, le Titulaire applique une mesure de contournement et un correctif en respectant les délais précisés dans le CCTP.

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

#### **Exigence SECU\_MCS\_009**

Lorsque le Titulaire découvre une vulnérabilité grave ou majeure au cours du MCS, une nouvelle version des composantes du système impactées est générée puis livrée.

#### **Exigence SECU\_MCS\_010**

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

#### **Exigence SECU\_MCS\_011**

Le Titulaire analyse pour toute modification d'un des systèmes de l'administration 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.

#### **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'administration. Les différents scénarii de tests sont détaillés dans le PMCS.

#### **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 (Par exemple : Procès-Verbal de livraison signé).

#### **Exigence SECU\_MSCS\_014**

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

#### **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, comprenant également le DAVR.

#### **Exigence SECU\_MCS\_016**

Le Titulaire identifie, au titre du MCS, les 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).

#### **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.

#### **Exigence SECU\_MCS\_018**

Le Titulaire prend en compte la gestion des correctifs de sécurité dans l'outil de gestion de configuration.

#### **Exigence SECU\_MCS\_019**

Le Titulaire garantit que la maintenance des logiciels assure la protection des informations et l'intégrité des systèmes de l'administration.

#### **Exigence SECU\_MCS\_020**

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

#### **Exigence SECU\_MCS\_021**

Pour les systèmes hébergés dans les locaux de l'administration, celle-ci met à disposition du Titulaire un outil de MCS remontant les vulnérabilités identifiées par le CERT-FR. Leur traitement (contournement ou correction) reste à la charge du Titulaire et est réalisé dans un délai correspondant à un niveau de risque (criticité) décidé en partenariat avec l'administration.

#### **Exigence SECU\_MCS\_022**

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'administration précisant au minimum :

- Un résumé de l'attaque et ses impacts potentiels ;
- Le vecteur d'attaque ;
- L'adresse IP de l'attaquant ;
- Les impacts de l'attaque sur l'écosystème de l'administration (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 précédemment.

## **6 EXIGENCES RELATIVES AUX DROITS D'ACCES**

#### **Exigence SECU\_ACCES\_001**

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

#### **Exigence SECU\_ACCES\_002**

Le Titulaire doit uniquement donner les droits d'accès à une application qu'aux fichiers qu'elle est légitime d'accéder.

#### **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 strictement nécessaires et suffisants.

#### **Exigence SECU\_ACCES\_004**

Les postes d'administration permettant l'accès aux environnements de l'administration depuis le site du titulaire doivent respecter les exigences suivantes (en suivant, à défaut d'une précision de l'administration, 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 pôle SSI de l'administration ;
- Les postes ne doivent pas avoir accès à internet, un intranet mutualisé ou une messagerie quelconque ;
- Les postes d'administration utilisés doivent être réservés exclusivement aux activités rendus à l'administration. 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 ;
- La connexion au site se fait obligatoirement au travers d'un VPN IPSEC.

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

## 7 EXIGENCES RELATIVES AUX PERSONNELS

### 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.

### Exigence SECU\_PERS\_002

Le Titulaire accepte d'effectuer les enquêtes sur le casier judiciaire (demande du bulletin n°3) de tous les membres des équipes de développement, d'intégration, de maintenance et d'exploitation.

### Exigence SECU\_PERS\_003

Le titulaire a obligation de communiquer mensuellement au pôle sécurité de l'administration 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 à la connaissance du pôle sécurité de l'administration sans délai. A défaut, un état de lieux annuel de cette liste sera adressé à la date anniversaire de la signature du marché.

### 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.

## 8 EXIGENCES RELATIVES A L'HEBERGEMENT ET L'EXPLOITATION PAR UN TIERS

### Exigence SECU\_HEB\_001

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

- 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.

### Exigence SECU\_HEB\_002

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

### **Exigence SECU\_HEB\_003**

Le Titulaire doit mettre en place les mesures adéquates pour assurer la continuité des services rendus par le système sous sa responsabilité conformément au besoin identifié dans l'analyse de risques.

## **9 ANNEXE 1 : EXIGENCES DE SECURITE GLOBALE**

Les Politiques de Sécurité des Systèmes d'Information de l'administration sont réputées connues du titulaire comme de ses agents qu'il aura déclarée à l'administration préalablement à tout commencement d'exécution du marché (Cf. SECU\_PERS\_003). Le titulaire s'engage à respecter, et faire respecter par ses personnels, l'ensemble des obligations de ces PSSI.

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'administration de toute difficulté dans l'application de ces mesures, de fuite ou de suspicion de fuite d'informations sensibles qu'il rencontre ou constate.

### **9.1 CLAUSE DE CONFIDENTIALITE**

Les supports informatiques fournis par l'administration et tous documents de quelque nature qu'ils soient résultant de leur traitement par le Titulaire restent la propriété de l'administration.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal).

Conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informations, aux fichiers et aux libertés, 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, c'est-à-dire notamment à :

- 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'administration ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées dans le lot 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.

Et en fin de marché, à :

- Procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations, et fournir les procès-verbaux de destruction correspondants ;

- Restituer intégralement les supports d'informations selon les modalités prévues dans les différents lots du marché.

A ce titre, le titulaire ne pourra 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.

L'administration se réserve le droit de procéder à toute vérification, après un préavis de cinq (5) jours ouvrés, qui lui paraîtrait utile pour constater le respect des obligations précitées par le Titulaire. (Cf. Exigence SECU\_DOS\_011).

Il est rappelé que, 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.

L'administration pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

## **9.2 CLAUSE DE SECURITE APPLICABLE A L'ACCES AUX LOCAUX**

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'administration doit être préalablement nommé agréé selon la procédure en vigueur et décrite dans la PSSI applicable.

Tout personnel 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 applicables. L'administration 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 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 cinq (5) jours ouvrés et il est fait obligation au titulaire de fournir à l'administration une photocopie lisible et recto-verso d'un document officiel d'identité.

## **9.3 PROTECTION DES INFORMATIONS SENSIBLES**

Par défaut, toutes les informations du Ministère de l'intérieur doivent être considérées comme sensible et à ce titre bénéficient des obligations de confidentialité prévues à l'article 5 du CCAG applicable au type de marché contractualisé.

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. Tout élément du dossier de sécurité d'un système est systématiquement considéré comme « Diffusion Restreinte ».

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.

Toute information sensible dont le titulaire a connaissance à l'occasion de l'exécution du marché ne peut en aucun cas être communiquée à un tiers (autre que les agents du titulaire préalablement



déclarés et autorisés par l'administration dans la Liste) sans accord préalable exprès et écrit de l'administration.

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

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

#### 9.3.1 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 identifiés :

- 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 des documents, celle-ci doit être réalisée par broyage ou incinération. 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.

#### 9.3.2 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 de l'administration. 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'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<sup>1</sup> : seuls les agents 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).

#### **9.4 CLAUSE RELATIVE A LA RESTITUTION DES INFORMATIONS**

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 à l'administration sans délai et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles.

#### **9.5 CLAUSE RELATIVE A LA SECURITE 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, leurs supports 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.

---

<sup>1</sup> Le besoin d'en connaître désigne la nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise.