

Annexe 1 CCTP : Obligations du titulaire et exigences de sécurité

1. Obligations du Titulaire dans le processus d'homologation des SI

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

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

Le Titulaire participe pour chaque projet à la constitution d'un dossier d'homologation présentant les données et leurs traitements, les mesures générales et particulières de sécurité, les moyens de protection associés ainsi que les moyens et techniques concourant au fonctionnement du système d'information. Le titulaire devra aider à la constitution pour recenser les vulnérabilités résiduelles et établir un plan d'action couvrant les différentes vulnérabilités afférentes à son domaine d'intervention.

Exigence SECU_HOM_001 Le Titulaire assiste le bénéficiaire dans l'élaboration de l'analyse de risques du système en vue d'identifier les risques auxquels l'application est confrontée en prenant en compte les potentiels impacts sur la vie privée des personnes dont les données font l'objet d'un traitement par le système d'information cible.

Exigence SECU_HOM_002 Le Titulaire réalise et met à jour les dossiers d'architecture technique de tous les systèmes d'information sur lesquels il intervient pour le compte du bénéficiaire. Chaque dossier d'architecture technique traite systématiquement des points suivants :

- Détail de l'architecture fonctionnelle : description des échanges métiers permettant au système de remplir sa mission ;

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

Exigence SECU_HOM_003 Le Titulaire doit justifier dans le DAT les mécanismes de sécurité mis en place dans la solution en vue de répondre aux objectifs de sécurité identifiés dans l'analyse de risque. Ces objectifs peuvent être satisfaits par un logiciel personnalisé, un logiciel tiers ou l'environnement technique de la solution.

Exigence SECU_HOM_004 Le Titulaire doit se conformer aux différentiels référentiels applicables selon les produits (NIS2, HDS, SNDS,...) et leurs domaines d'application.

2. Obligations du Titulaire sur le maintien en condition de sécurité (MCS)

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 la conception et tout au long de la vie du système.

Exigence SECU_MCS_001 Le Titulaire veille à fournir selon leur périmètre d'intervention les solutions de lutte contre les codes malveillants utilisés sur les systèmes des différents projets du bénéficiaire 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 le bénéficiaire. Le Titulaire s'assure que les postes de travail ainsi que les serveurs transverses du bénéficiaire soient dotés de procédures permettant de sécuriser les postes et les serveurs.

Exigence SECU_MCS_002 Le Titulaire met en œuvre une veille de sécurité pour l'ensemble des produits (logiciels et matériels) du bénéficiaire, 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.

Exigence SECU_MCS_003 En cas de mise en évidence d'une vulnérabilité affectant un système du bénéficiaire relevant du marché, le Titulaire collabore avec le bénéficiaire 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 sécurités observées 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.

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 du bénéficiaire (ou un représentant habilité par le bénéficiaire) 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).

Exigence SECU_MCS_005 Au titre de la requalification de la note CVSS et 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 le bénéficiaire de la note environnementale sauf décision contraire de l'autorité d'homologation du système.

Exigence SECU_MCS_006 Au titre de la requalification de la note CVSS et pour les vulnérabilités de criticité « Moyen » découvertes au titre du MCS, le Titulaire :

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

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

Exigence SECU_MCS_007 Au titre de la requalification de la note CVSS et pour les vulnérabilités de criticité « Elevé » découvertes au titre du MCS, le Titulaire :

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

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

Exigence SECU_MCS_008 Au titre de la requalification de la note CVSS et pour les vulnérabilités de criticité « Critique » découvertes au titre du MCS, le Titulaire :

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

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

Exigence SECU_MCS_009 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).

Exigence SECU_MCS_010 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).

3. Obligations du Titulaire sur la gestion des biens du bénéficiaire

Exigence SECU_GDB_001 Le Titulaire conserve et traite les données du bénéficiaire de manière séparée de ses propres données ou de données d'autres clients du Titulaire. Le Titulaire doit restreindre l'accès aux données du bénéficiaire suivant le principe de restriction au besoin d'en connaître.

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.

Exigence SECU_GDB_003 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.

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

Les exigences SECU_SRE seront adaptés en fonction des projets du SI du titulaire en fonction de sa responsabilité. Les postes de travail ou les infrastructures du Titulaire seront soumis à ces règles.

Exigence SECU_SRE_001 Le Titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

Exigence SECU_SRE_002 Le Titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Le Titulaire doivent respecter les exigences suivantes (en suivant, à défaut d'une précision du bénéficiaire, les recommandations de l'ANSSI) :

- Les correctifs de sécurité et les mises à jour antivirus doivent se faire régulièrement (correctif Windows mensuel, MAJ antiviral quotidienne...) ;

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 le bénéficiaire. Toute exception fera l'objet d'un accord préalable écrit des équipes du bénéficiaire. A ce titre, les mots de passe hérités des paramétrages d'usine des produits doivent systématiquement être modifiés lors du durcissement de leur configuration pour les besoins du bénéficiaire. Le titulaire utilisera des guides de hardenning (par exemple CIS Security)

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 le bénéficiaire. Le Titulaire s'assurera de la conformité des postes au niveau sécurité, et que les utilisateurs n'aient pas le droit d'administration. L'ensemble des demandes autour des postes doivent être tracées et soumis à un processus de dérogation le cas échéant. Le bénéficiaire devra être consulté pour toutes dérogations pouvant affecter son Système d'Information.

Exigence SECU_SRE_005 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 le bénéficiaire) dispose d'un compte individuel qui doit être un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte.

- Un n compte de service pourra être utilisé pour l'utilisation des produits. Il devra être soumis à des règles strictes et non utilisé par le personnel du Titulaire

Exigence SECU_SRE_006 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.

Exigence SECU_SRE_007 Le Titulaire doit fournir un inventaire justifié des comptes individuels ou de service (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système. Il devra suivre régulièrement les comptes (renouvellement des mots de passes des comptes techniques).

Exigence SECU_SRE_008 Le Titulaire tient à jour la liste exhaustive des comptes d'accès au SI du bénéficiaire existants ainsi que des rôles et privilèges qui y sont associés. Il fournit cette liste à le bénéficiaire 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.

Exigence SECU_SRE_009 Le Titulaire met en œuvre les bonnes pratiques de définition des mots de passe de l'ANSSI sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du Titulaire.

Exigence SECU_SRE_010 Le Titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par le bénéficiaire.

Exigence SECU_SRE_011 Le Titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou du bénéficiaire dans le cadre de la prestation.

Exigence SECU_SRE_012 Le Titulaire est capable de fournir au bénéficiaire, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI du bénéficiaire en astreinte.

Exigence SECU_SRE_013 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 du bénéficiaire précisant a minima :

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

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

5. Obligations du titulaire sur la sécurité de ses postes de travail

Exigence SECU_SPT_001 En vue de prévenir le vol des données du bénéficiaire contenues dans les postes de travail nomade du Titulaire, celui-ci met systématiquement en place les mesures de protection suivantes :

- Utilisation d'un filtre de confidentialité lors de déplacement ou d'utilisation de postes en espace partagé ;
- Installation d'une solution de chiffrement surfacique pour limiter le risque en cas de vol du matériel

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 les quinze minutes.

Exigence SECU_SPT_003 Tous les postes de travail du Titulaire doivent disposer d'une solution de chiffrement robuste, en privilégiant les solutions qualifiées par l'ANSSI, afin de permettre le chiffrement des données sensibles du bénéficiaire que les personnels du Titulaire seraient amenés à stocker ou communiquer dans le cadre de leurs missions.

6. Obligations du titulaire sur le traitement des incidents de sécurité

Exigence SECU_INC_001 Le Titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

Exigence SECU_INC_002 Le Titulaire contacte les interlocuteurs sécurité du bénéficiaire désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI du bénéficiaire :

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

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

Exigence SECU_INC_003 Le Titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit au bénéficiaire sur demande.

7. Obligations du Titulaire lors de l'accès aux locaux du bénéficiaire

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 du

bénéficiaire doit être nommément agréé selon la procédure en vigueur dans les locaux du bénéficiaire.

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

Exigence SECU_AL_002 L'intervention dans les zones protégées du bénéficiaire 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 au bénéficiaire :

- Les données d'état civil 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.

8. Obligations du Titulaire intervenant au sein des locaux du bénéficiaire

Exigence SECU_TIERS_001 Au même titre que les agents du bénéficiaire, le Titulaire doit prendre connaissance et appliquer les référentiels internes du bénéficiaire (politiques de sécurité numérique, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, ...).

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.

Exigence SECU_TIERS_003 Le Titulaire élabore et maintient un inventaire complet et à jour des matériels mis à sa disposition par le bénéficiaire. Cette liste doit être transmise semestriellement au responsable désigné par le bénéficiaire.

Exigence SECU_TIERS_004 Le Titulaire tient à jour la liste exhaustive des comptes d'accès aux systèmes d'information du bénéficiaire existants ainsi que des rôles et privilèges qui y sont associés. Il doit être en mesure de fournir cette liste à le bénéficiaire sur demande. Le Titulaire doit également effectuer et formaliser une revue trimestrielle des comptes d'accès aux serveurs et autres ressources du bénéficiaire utilisées par le Titulaire dans le cadre de la prestation.

9. Obligations du Titulaire sur le nomadisme numérique

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

Exigence SECU_NOMADE_001 Dans le cas où le bénéficiaire autorise formellement les accès distants vers ses systèmes d'information et ne fournit pas directement les moyens pour cette activité, 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.

Exigence SECU_NOMADE_002 Le Titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex : VPN IPSec) pour la connexion à distance aux réseaux utilisés dans le cadre de la Prestation (que ce soient ceux du Titulaire, ceux du bénéficiaire ou les deux éventuellement). Le personnel du Titulaire devra explicitement lancer la connexion et s'authentifier pour obtenir l'accès à distance aux SI du bénéficiaire (connexion authentifiée non permanente) ou utiliser les services et moyens d'accès distants mis à disposition par le bénéficiaire.

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.

Exigence SECU_NOMADE_004 Le Titulaire devra être conforme aux recommandations sur le nomadisme numérique de l'ANSSI.

10. Obligations en cas d'interconnexion avec les SI du Titulaire

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

Exigence SECU_INTERCO_001 Le Titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation. Il doit remonter au plus tôt au bénéficiaire toute anomalie lui permettant d'accéder de manière privilégiée à des ressources qui ne relèvent pas de sa responsabilité.

Exigence SECU_INTERCO_002 En cas d'interconnexion des SI du bénéficiaire et du Titulaire, le Titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par le bénéficiaire au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité du bénéficiaire.

Exigence SECU_INTERCO_003 Pour chaque interconnexion, les éléments suivants doivent être précisés dans la cartographie :

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

11. Obligations du Titulaire sur la sécurité des développements

Exigence SECU_DEV_001 Le Titulaire doit prioriser les logiciels du cadre de cohérence technique du bénéficiaire ou du catalogue de l'ANSSI.

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).

Exigence SECU_DEV_003 La sécurité de toutes les applications développées par le Titulaire doit être systématiquement validée par des audits automatiques de sécurité visant à identifier les vulnérabilités potentielles sur le code et ses dépendances. Les règles d'exception mis en place par le Titulaire seront étudiées/validées avec le bénéficiaire.

Exigence SECU_DEV_004 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 du bénéficiaire, ne soient accidentellement inclus dans la solution au cours des développements.

Exigence SECU_DEV_005 Le Titulaire doit utiliser un système de contrôle du code source qui authentifie les personnels contributeurs et journalise toutes les modifications au produit de base du logiciel.

Exigence SECU_DEV_006 Le Titulaire doit garantir que les environnements de développement, de qualification, de préproduction seront séparés de manière logique et/ou physique de la plateforme de production.

Exigence SECU_DEV_007 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. Dans le cas, ou il n'est pas possible d'anonymiser complètement les données, le Titulaire précisera les modalités de transfert sécurisé avec les processus associés et de suivi. Les processus devront être décrits dans le PAS. Les plateformes hors production recevant des données issues de la production devront être considérées avec un niveau de sécurité équivalent à la production et être auditées par le Titulaire (Comptes nominatifs limités, accès par MFA....). Les dumps pourront être considérés comme données sensibles (en fonction du niveau de la sécurité du produit). La durée de conservation doit être limitée et conforme aux règles du RGPD. En fonction du niveau de sensibilité des données, le processus sera soumis à la validation du bénéficiaire.

Exigence SECU_DEV_008 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 du bénéficiaire 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.

Exigence SECU_DEV_009. Le titulaire doit mettre en place des contrôles de conformité par rapport aux exigences définies. Ceux-ci seront définis avec le bénéficiaire afin de pouvoir les récolter automatiquement pour produire un rapport centralisé dans les outils du bénéficiaire.

12. Obligations du titulaire sur la gestion des droits d'accès

Exigence SECU_ACCES_001 Le Titulaire doit mettre en place sur l'ensemble du parc de serveurs du bénéficiaire, des comptes d'accès nominatifs. Les droits des personnels d'exploitation doivent être limités au strict nécessaire pour la bonne réalisation de leurs missions.

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 le DAT du système d'information les règles de durcissements mises en œuvre pour s'assurer du respect de cette exigence.

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.

13. Obligations du titulaire en matière de continuité d'activité

Exigence SECU_PCA_001 Pour chaque système d'information dont il a la charge dans le cadre du marché, le Titulaire assiste le bénéficiaire dans la réalisation du bilan d'impact sur l'activité des systèmes d'information du bénéficiaire sur lesquels il intervient.

Exigence SECU_PCA_002 Le Titulaire effectue au moins annuellement des tests de restauration des sauvegardes effectuées sur les données des systèmes d'information du bénéficiaire qu'il exploite en son nom.

14. Obligations du titulaire en matière de gestion du personnel

Exigence SECU_GPE_001. Le personnel doit être sensibilisé et formé en fonction de son périmètre d'information sur la sécurité (ex OWASP)

Le Titulaire devra sensibiliser régulièrement le personnel sur les nouvelles tendances de sécurité. Il devra rappeler les clauses du PAS.