



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – E01

**Clauses de sécurité types des marchés publics
ou accords-cadres**

Version 1.0

TABLES DES MATIERES

1.	Prise en main du document	5
2.	Clauses à intégrer dans le RC	6
2.1.	Exigences de sécurité du Plan d'Assurance Sécurité	6
2.2.	Formulaire d'engagement de reconnaissance de responsabilité	6
2.3.	Sous-traitance.....	7
2.4.	Hébergement des données et des services	7
3.	Clauses à intégrer dans le CCAP	9
3.1.	Dossier d'homologation	9
3.2.	Devoirs du Titulaire en matière de conseil et de conformité à l'état de l'art.....	10
3.3.	Cartographie des systèmes d'information	10
3.4.	Protection de l'information	11
3.5.	Maintien en condition de sécurité	12
3.6.	Information sur les événements et incidents de sécurité	13 ¹²
3.7.	Gestion du personnel	13
3.8.	Sécurisation des locaux du Titulaire.....	15 ¹⁴
3.9.	Propriété intellectuelle des résultats	15
3.10.	Echéance ou résiliation du marché	16 ¹⁵
3.11.	Réversibilité	16
3.12.	Audit de sécurité sur le périmètre du Titulaire	17 ¹⁶
3.13.	Pénalités	18 ¹⁷
4.	Clauses à intégrer dans le CCTP	19¹⁸
4.1.	Obligations du Titulaire dans l'homologation des SI.....	19 ¹⁸
4.2.	Obligations du Titulaire sur le maintien en condition de sécurité.....	21 ²⁰
4.3.	Obligations du Titulaire à se conformer à l'Etat de l'art	23
4.4.	Obligations du Titulaire sur la gestion des biens de l'Acheteur.....	24 ²³
4.5.	Obligations du Titulaire sur la sécurité de ses locaux informatiques	25
4.6.	Obligations du titulaire sur la sécurité des réseaux et de l'exploitation	27 ²⁶
4.7.	Obligations du titulaire sur la sécurité de ses postes de travail	29 ²⁸
4.8.	Obligations du titulaire sur le traitement des incidents de sécurité	30 ²⁹
4.9.	Obligations du Titulaire lors de l'accès aux locaux de l'Acheteur.....	30
4.10.	Obligations du Titulaire intervenant au sein des locaux de l'Acheteur	31 ³⁰
4.11.	Obligations du Titulaire sur le nomadisme numérique.....	32 ³¹

4.12. Obligations en cas d'interconnexion avec les SI du Titulaire	32 <u>31</u>
4.13. Obligations du Titulaire sur les prestations d'Etude	33 <u>32</u>
4.14. Obligations du Titulaire sur la sécurité des développements.....	33 <u>32</u>
4.15. Obligations du Titulaire sur les achats de services, matériels ou logiciels.....	36 <u>35</u>
4.16. Obligations du titulaire sur la gestion des droits d'accès.....	37
4.17. Obligations du Titulaire dans la gestion des personnels.....	38 <u>37</u>
4.18. Obligations du titulaire en matière de continuité d'activité.....	38
5. Annexes	40<u>39</u>
5.1. Glossaire	40 <u>39</u>
5.2. Attestation de reconnaissance de responsabilité (2 pages)	43 <u>42</u>
5.3. Identification des exigences applicables à l'objet du marché	45 <u>44</u>

Préambule

Le présent document a vocation à établir et mettre à disposition des services en charge de la rédaction des marchés, une base solide d'exigences de sécurité types.

Il liste ainsi les exigences de sécurité à intégrer dans les différentes pièces d'un marché ou d'un accord-cadre :

- Règlement de consultation (RC) ;
- Cahier des Clauses Administrative Particulière (CCAP) ;
- Cahier des Clauses Techniques Particulières (CCTP).

Il a ainsi pour objectif de fournir aux Acheteurs (qu'ils soient rédacteurs, juristes, prescripteurs métier ou technique, ...) une liste des exigences de sécurité types à intégrer dans le dossier de consultation des entreprises (DCE) des marchés publics.

1. Prise en main du document

Le présent document n'a pas pour objectif d'établir une liste exhaustive des exigences de sécurité applicable, sans discernement, à n'importe quel marché du ministère. Il tend à réunir dans un seul l'ensemble des exigences susceptibles d'être applicable à un marché et permettre ainsi aux différents Acheteurs de disposer d'une base solide dans la conception de leur cahier des charges sécuritaire.

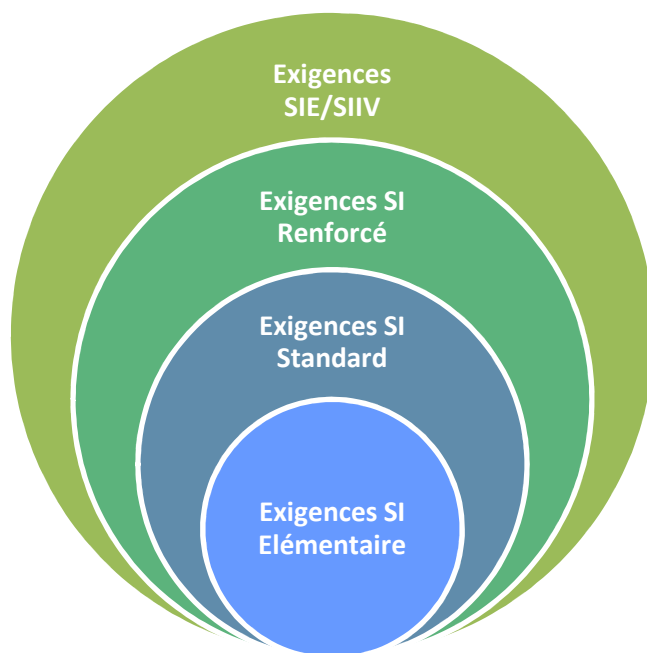
Chaque liste du présent document devra donc être analysée, en lien avec les acteurs SSI concernés, afin de déterminer si elles sont applicables :

- A l'objet du marché : Le partie 5.3 en annexe du présent document permet de faire un premier filtre des exigences applicables en fonction de l'objet du marché.
- Aux enjeux des systèmes d'information cible : Pour les marchés regroupant plusieurs système d'information, il convient de considérer le plus critique pour déterminer les exigences applicables.
- Aux risques ciblant les systèmes d'information : Dans le cas où une analyse de risque a été réalisé antérieurement au marché, il conviendra d'établir la correspondance entre les exigences du présent document et les mesures identifiées. Le cas échéant, des mesures spécifiques devront être ajoutées pour pleinement intégrer les recommandations de l'analyse de risque.

Lorsque l'objet ou les livrables du marché relèvent d'une réglementation pouvant avoir des conséquences aussi bien pour le Titulaire que pour l'Acheteur (notamment protection du secret de défense, protection des infrastructures vitales), les Acheteurs sont invités à mentionner ces réglementations dans les documents de la consultation et à se rapprocher au préalable de leur chaîne fonctionnelle en charge de la sécurité des systèmes d'information.

Le présent document doit être amendé afin d'inclure ou détailler les réglementations spécifiques (IGI 1300, II 901, RGPD, ...), les documents contractuels applicables (politiques et procédures de sécurité de l'Acheteur, ...) ou toutes autres dispositions nécessaires à la sécurisation des prestations couvertes par le marché.

Pour faciliter cette prise en main, un document complémentaire sera mise à disposition des Acheteurs et leur permettra de faciliter l'identification des exigences applicables au marché ciblé et ainsi d'associer à chaque niveau identifié dans la démarche d'intégration de la sécurité des systèmes d'information dans les projets et en fonction de l'objet du marché, la liste des exigences applicables pour une couverture des risques nécessaires. Toute entité est responsable de la suffisance des mesures sélectionnées.



2. Clauses à intégrer dans le RC

2.1. Exigences de sécurité du Plan d'Assurance Sécurité

2.1.1. RC-Exigence SECU_PAS_001

Le Titulaire doit rédiger un Plan d'Assurance Sécurité (PAS) précisant les engagements de ce dernier pour répondre aux exigences de sécurité du marché et les moyens qu'il mettra en œuvre pour assurer que les livrables produits respectent les exigences de sécurité du marché.

2.1.2. RC-Exigence SECU_PAS_002

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

2.1.3. RC-Exigence SECU_PAS_003

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

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

Note : L'obligation de respecter les exigences applicables de la politique de sécurité numérique de l'Acheteur doit être indiquée dans le CCAP et figurer dans la liste des documents contractuels.

2.1.4. RC-Exigence SECU_PAS_004

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

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

2.1.5. RC-Exigence SECU_PAS_005

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

2.1.6. RC-Exigence SECU_PAS_006

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

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

2.2. Formulaire d'engagement de reconnaissance de responsabilité

2.2.1. RC-Exigence SECU_ERR_001

Le Titulaire confirme avoir pris connaissance des règles de sécurité à appliquer en signant le formulaire d'engagement et de reconnaissance de responsabilité joint en annexe.

Note : L'engagement peut figurer, le cas échéant, dans la liste des documents contractuels visés dans le CCAP.

2.3. Sous-traitance

En matière de marchés publics, la sous-traitance est l'opération par laquelle le Titulaire d'un marché confie à un opérateur tiers l'exécution d'une partie des prestations qui lui ont été confiées par l'Acheteur.

Les obligations du Titulaire, y compris les clauses de sécurité, s'appliquent intégralement à ses sous-traitants et sont sous sa responsabilité.

2.3.1. RC-Exigence SECU_ST_001

En application des CCAG, le Titulaire doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché et doit s'assurer du respect de ces obligations par ses sous-traitants.

Cas d'autorisation de sous-traitance des tâches essentielles :

L'Acheteur n'exige pas que certaines tâches essentielles soient effectuées directement par le Titulaire.

Cas d'interdiction de sous-traitance des tâches essentielles :

Les tâches essentielles stipulées dans le règlement de consultation du marché doivent être exécutées directement par le Titulaire et ne peuvent faire l'objet d'aucune sous-traitance : [A compléter par l'Acheteur]

Note : La liste des tâches essentielles peut également être indiquée directement dans l'appel d'offre à la concurrence.

2.4. Hébergement des données et des services

En fonction de la sensibilité des données ou des services qui seront confiés au Titulaire, l'Acheteur peut demander aux soumissionnaires des précisions sur la localisation et l'hébergement des données ou des services liés à la prestation.

2.4.1. RC-Exigence SECU_HEB_001

Le soumissionnaire précise dans son offre les lieux géographiques dans lesquels :

- Les données informatiques liées à la prestation seront hébergées ;
- Les services objets de la prestation seront localisés ;
- Les systèmes d'accès et d'administration des services liés à la prestation seront localisés.

2.4.2. RC-Exigence SECU_HEB_002

Le soumissionnaire précise dans son offre si ses infrastructures (techniques ou organisationnelles) sont gérées ou simplement accessibles par une entité juridique appartenant à un pays disposant de lois autorisant ce pays à accéder aux données.

Le soumissionnaire décrit, le cas échéant, les risques environnementaux dont font l'objet les sites hébergeant les données ou du service et précise dans un plan de prévention des risques (PPR) les mesures mises en œuvre pour couvrir ces risques.

2.4.3. RC-Exigence SECU_HEB_003

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

- Les attaques classiques sur IP et les protocoles associés (Par exemple : Attaque de type déni de service).
- Les codes malveillants pouvant affecter la disponibilité, compromettre la sécurité ou consommer de manière excessive les ressources de l'application.

Ces mécanismes/outils doivent être détaillés dans le PAS.

2.4.4.RC-Exigence SECU_HEB_004

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

2.4.5.RC-Exigence SECU_HEB_005

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

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

3. Clauses à intégrer dans le CCAP

Les marchés peuvent faire référence à d'autres Cahiers des Clauses Administratives Générales (CCAG) que le CCAG-TIC. Le CCAG choisi dépend de l'objet du marché public.

Dans un souci de simplicité, le présent document fera référence au CCAG-TIC. L'Acheteur devra donc adapter les clauses types en fonction du CCAG choisi.

Des clauses spécifiques du CCAP peuvent venir compléter ce corpus afin d'être plus adaptées au cas du marché public ou de l'accord cadre.

3.1. Dossier d'homologation

Le dossier d'homologation comprend des documents contractuels permettant d'attester que le soumissionnaire a mis en œuvre une démarche de gestion des risques et qu'il appliquera les exigences de sécurité de l'Acheteur. A ce titre, les documents qui composent un dossier d'homologation doivent être listés parmi les pièces contractuelles du marché en complément de l'article 4 du CCAG-TIC.

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

- L'analyse des risques numériques du SI ;
- Bilan d'impact sur l'activité (BIA) ;
- Le rapport d'audit de sécurité du SI ;
- Le dossier d'architecture technique (DAT) ;
- La Procédure de Gestion des Incidents de sécurité (PGI)
- La Procédure d'Exploitation de Sécurité (PES) ;
- Le Plan de Maintien en Condition de Sécurité (PMCS) ;
- Plan d'Assurance Sécurité (PAS) ;
- Les attestations de certification / qualification des produits ou services ;
- Le plan de remédiation.

Nom du livrable	Délai de livraison
Analyses des risques numériques des SI	Avant mise en production et en tant que de besoin en fonction du planning d'homologation du système.
Bilan d'Impact sur l'Activité (BIA)	Avant la mise en production pour les nouveaux SI. T0 + 6 mois et en tant que de besoin en cas d'évolution des besoins en disponibilité
Dossier d'Architecture Technique (DAT)	Avant mise en production et en tant que de besoin en cas d'évolution du système
Plan d'Assurance Sécurité (PAS)	T0 + 1 mois et en tant que de besoin en cas d'évolution des exigences
Plan de maintien en conditions de sécurité (PMCS)	T0 + 3 mois et en tant que de besoin en cas d'évolution du système
Plan de remédiation	T0 + 15 jours après rédaction de l'analyse de risques ou après toute réunion de restitution d'un audit
Procédure d'exploitation de sécurité (PES)	T0 + 2 mois et en tant que de besoin en cas d'évolution du système

Nom du livrable	Délai de livraison
Procédure de gestion des incidents de sécurité (PGI)	T0 + 3 mois et en tant que de besoin en cas d'évolution du système ou lors du processus de capitalisation sur les événements rencontrés
Rapports d'audit de sécurité	Avant la mise en production des nouveaux SI et tous les 2 ans après la livraison du premier rapport T0 + 6 mois pour les SI déjà en production et tous les 2 ans après la livraison du premier rapport
Attestations de certification / qualification des produits ou services.	A chaque livraison d'un dossier d'homologation ou sur demande de l'Acheteur.

3.2. Devoirs du Titulaire en matière de conseil et de conformité à l'état de l'art

3.2.1. CCAP-Exigence SECU_CEA_001

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

3.2.1. CCAP-Exigence SECU_CEA_002

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

3.2.1. CCAP-Exigence SECU_CEA_003

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

3.3. Cartographie des systèmes d'information

En fonction de l'objet du marché, des enjeux financiers, de la complexité, et de la sensibilité des données, il est recommandé que l'Acheteur établisse la cartographie complète de ses SI.

Nom du livrable	Délai de livraison
Cartographie des SI	T0 + 6 mois et en tant que de besoin en cas d'évolution du système. T0 correspond à la date de validation du modèle de cartographie par l'Acheteur. Le modèle doit être fourni au plus tard 30 jours après le début du marché.

3.3.1.CCAP-Exigence SECU_CARTO_001

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

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

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

3.4. Protection de l'information

3.4.1.CCAP-Exigence SECU_PDI_001

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

Note : L'Acheteur peut rendre contractuels des documents en fonction de ses besoins ou du cadre légal en vigueur. Pour ce faire, il devra compléter la clause en listant les documents contractuels applicables au marché ou à l'accord cadre, par exemple :

- *Données classifiées au sens de l'IGI 1300 : En cas de manipulation d'informations classifiées de défense, le Titulaire respecte les exigences de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense.*
- *Données portant la mention « Diffusion Restreinte » : Les informations de niveau « Diffusion Restreinte » (DR) doivent être protégées conformément à l'instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles.*
- *Données à caractère médical : Article L. 1111-8 du code de la santé publique sur l'hébergement des données de santé.*
- *Données de recherche, données stratégiques et techniques : Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation, arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.*
- *Données à caractère personnel : Règlement (UE) 2016/679 du parlement européen et conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) dit RGPD.*

3.4.2.CCAP-Exigence SECU_PDI_002

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

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

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

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

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

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

3.4.3. CCAP-Exigence SECU_PDI_003

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

3.4.4. CCAP-Exigence SECU_PDI_004

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

3.4.5. CCAP-Exigence SECU_PDI_005

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

3.5. Maintien en condition de sécurité

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

3.5.1. CCAP-Exigence SECU_MCS_001

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

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

3.5.2. CCAP-Exigence SECU_MCS_002

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

3.5.3. CCAP-Exigence SECU_MCS_003

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

3.6. Information sur les évènements et incidents de sécurité

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

3.6.1. CCAP-Exigence SECU_EIS_001

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

3.6.1. CCAP-Exigence SECU_EIS_002

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

3.7. Gestion du personnel

3.7.1. CCAP-EXIGENCE SECU_GDP_001

Le Titulaire doit désigner un responsable sécurité qui devient l'interlocuteur privilégié de l'Acheteur pour tous les sujets de sécurité et ce, durant toute la durée du marché.

L'Acheteur se réserve le droit de vérifier le niveau de compétences en matière de sécurité de ce responsable et de le récuser si elle juge ce niveau insuffisant, le Titulaire ayant alors l'obligation de proposer sans délai à l'Acheteur un nouveau candidat.

Il appartient à ce responsable sécurité de sensibiliser les agents du Titulaire, et de ses sous-traitants éventuels, pour un strict respect des obligations en matière de SSI et d'en présenter un bilan à l'occasion de la réunion de chaque comité de pilotage du marché.

Le responsable sécurité du Titulaire établit un annuaire de contacts qu'il met à disposition de l'Acheteur sur demande.

3.7.2. CCAP-Exigence SECU_GDP_002

Le Titulaire a obligation de communiquer à 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 à la connaissance de l'Acheteur sans délai. A défaut, un état de lieux annuel de cette liste sera adressé à l'Acheteur à la date anniversaire de la signature du marché.

La liste élaborée par le Titulaire doit être systématiquement transmise au responsable projet, à l'officier de sécurité et/ou le conseiller de la sécurité numérique de l'Acheteur.

3.7.3. CCAP-Exigence SECU_GDP_003

Le Titulaire reconnaît avoir fait signer par tous ses agents appelés sous sa responsabilité à un titre quelconque à intervenir pour le compte du Titulaire dans le cadre de l'exécution du marché, une attestation de reconnaissance de responsabilité (Cf. annexe) par laquelle lesdits agents attestent avoir pris connaissance des exigences et contraintes de sécurité imposées par l'Acheteur, ainsi que de la législation applicable.

Cette attestation doit être obligatoirement signée, après la notification du marché et avant tout commencement d'exécution, par les agents du Titulaire susceptibles d'intervenir dans le cadre des prestations du marché. En cas de sous-traitance, l'engagement de reconnaissance de responsabilité doit également être signé par les agents du sous-traitant et communiqué à l'Acheteur par le Titulaire.

Toutes les attestations de reconnaissance de responsabilité signées doivent être systématiquement transmises au responsable projet et l'acteur en charge de la sécurité numérique désignés par l'Acheteur.

Le Titulaire s'engage à ce que seules les personnes ayant préalablement souscrit l'attestation de reconnaissance de responsabilité précitée interviennent de quelque manière que ce soit dans l'exécution du marché.

3.7.4. CCAP-Exigence SECU_GDP_004

En cas de départ définitif d'une personne nommément désignée, affectée par le Titulaire à l'exécution des prestations du marché, le Titulaire doit :

- En aviser, sans délai, l'Acheteur et prendre toutes dispositions nécessaires, afin d'assurer la poursuite de l'exécution des prestations ;
- Proposer à l'Acheteur un remplaçant disposant de compétences au moins équivalentes et dont il lui communique le curriculum vitae dans un délai de trois (3) mois à compter de la date d'envoi de l'avis mentionné à l'alinéa précédent.

Le remplaçant proposé par le Titulaire est considéré comme accepté par l'Acheteur, si celui-ci ne le récusé pas dans le délai d'un mois courant à compter de la réception de la communication mentionnée ci-dessus. La décision de récusation prise par l'Acheteur est motivée. Si l'Acheteur récusé le remplaçant, le Titulaire dispose d'un délai de trois mois pour proposer un autre remplaçant.

A défaut de proposition de remplaçant par le Titulaire ou en cas de récusation motivée des remplaçants par l'Acheteur, et plus globalement en cas de non-respect de ses obligations contractuelles relatives au remplacement du personnel, le marché peut être résilié dans les conditions prévues à l'article 42.2 du CCAG-TIC.

3.7.5. CCAP-Exigence SECU_GDP_005

Pendant toute la durée d'exécution du marché, l'Acheteur se réserve le droit de récusé les membres du personnel qui s'avèreraient inadaptés à l'exécution des prestations sur la base des résultats correspondant à une période d'essai de trois mois. Il motive sa décision après concertation avec le Titulaire. Ce dernier procède au remplacement du personnel récusé dans les mêmes conditions que pour un départ définitif (Cf. exigence [SECU_GDP_004]). En aucun cas le remplacement du personnel ne peut justifier une augmentation des prix du marché.

3.7.6. CCAP-Exigence SECU_GDP_006

Le Titulaire sensibilise son personnel, intervenant dans le cadre des prestations du marché, à la sécurité de l'information, des systèmes d'information et aux règles spécifiques de l'Acheteur.

Le Titulaire veille notamment à ce que son personnel intervenant dans le cadre de des prestations respecte les dispositions concernant la sécurité du présent marché.

3.7.7. CCAP-Exigence SECU_GDP_007

Aucune dérogation sur la gestion des personnels ne pourra être acceptée ou exigée de l'Acheteur, y compris en vue de pourvoir au remplacement inopiné, fortuit ou même urgent d'un agent du Titulaire.

Le non-respect ou l'inobservation par le Titulaire de ces mesures de sécurité, même dans les cas où ils résultent d'une imprudence ou d'une négligence, peuvent entraîner des pénalités, sans préjudice des sanctions pénales applicables.

3.8. Sécurisation des locaux du Titulaire

3.8.1. CCAP-Exigence SECU_LOC_001

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

3.8.2. CCAP-Exigence SECU_LOC_002

A tout moment pendant l'exécution du marché, l'Acheteur se réserve le droit de réaliser tout contrôle, après un préavis de trois (3) jours ouvrés, dans les locaux du Titulaire pour vérifier que sont effectivement respectées les préconisations validées par l'Acheteur s'agissant des règles de gestion et des mesures techniques de sécurisation des moyens de traitement des informations sensibles du ministère.

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

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

3.9. Propriété intellectuelle des résultats

3.9.1. CCAP-Exigence SECU_PI_001

Le CCAG-TIC propose deux options pour les clauses de propriété intellectuelle, qui peuvent être complétées en fonction des besoins :

- **L'option A « Concession de droits d'utilisation sur les résultats »**, applicable par défaut, qu'il est conseillé de compléter dans le CCAP :
 - L'Acheteur souhaite exploiter les résultats pour ses besoins propres et que ne sont envisagés notamment ni une mutualisation avec des administrations non identifiées au stade de l'appel d'offre ni une diffusion sous licence libre. Cette option prévoit une concession des droits afférents aux résultats (qui s'apparente à une licence d'utilisation) pour les besoins qui découlent de l'objet du marché.
- **L'option B « Cession exclusive des droits du Titulaire au pouvoir adjudicateur »**, qui doit être obligatoirement complétée dans le CCAP sous peine que la cession des droits soit nulle :
 - Le Titulaire cède, à titre exclusif, les droits d'exploitation des résultats à l'Acheteur qui peut dès lors les exploiter et les rétrocéder à des tiers, pour les seuls modes d'exploitation prévus dans le marché. Dans cette option, le Titulaire ne peut plus, en raison de l'exclusivité, exploiter les résultats. Si l'Acheteur souhaite avoir une maîtrise totale quant à l'exploitation des résultats, cette option est la plus appropriée.

Le choix de l'option nécessite d'identifier les résultats (livrables) du marché, susceptibles d'être protégés par des droits de propriété intellectuelle et de déterminer les besoins en termes d'utilisation de ces résultats.

Note : Les clauses de propriété intellectuelle en lien avec les projets informatiques sont traitées plus en détail dans le guide « Achats informatiques et propriété intellectuelle » élaboré de manière conjointe par l'APIE, la Direction interministérielle du numérique de l'État (DINUM) et la Direction des Achats de l'État (DAE).

3.10. Echéance ou résiliation du marché

3.10.1. CCAP-Exigence SECU_ERM_001

En fin de marché ou en cas de résiliation, le Titulaire doit prémunir l'Acheteur contre toute interruption ou baisse de la qualité des services avant la fin dudit marché.

Le Titulaire assure également l'ensemble des opérations pour que l'Acheteur puisse reprendre les services dans de bonnes conditions (transfert de compétences, documentations, ...).

3.10.2. CCAP-Exigence SECU_ERM_002

L'Acheteur peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du Titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

3.10.3. CCAP-Exigence SECU_ERM_003

Au terme du marché ou en cas de résiliation, le Titulaire restitue sans délai à l'Acheteur une copie de l'intégralité des données qui lui ont été confiées (directement par l'Acheteur ou produit par le Titulaire pour le compte de l'Acheteur) dans le cadre de la prestation. Un procès-verbal de restitution doit être établi par le Titulaire qui identifie le représentant de l'Acheteur à qui sont remis les données sur support électronique et la liste des données remises.

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

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

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

3.10.4. CCAP-Exigence SECU_ERM_004

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

3.10.5. CCAP-Exigence SECU_ERM_005

En complément de l'article 42 du CCAG-TIC, en cas de non-respect avéré des règles de sécurité portant de graves préjudices aux actifs ou activités de l'Acheteur, l'Acheteur peut résilier pour faute le marché sans mise en demeure ou avec dans les conditions de l'article 42.2 du CCAG TIC.

3.11. Réversibilité

En fin de marché ou en cas de résiliation, le Titulaire doit prémunir l'Acheteur contre toute interruption ou baisse de la qualité des services avant la fin dudit marché. Dans le cas où un PAS est demandé, il conviendra d'exiger que cette phase de réversibilité soit décrite par le Titulaire dans ce document. Dans le cas contraire, l'Acheteur doit prévoir les modalités de réversibilité dans le CCTP.

3.11.1. CCAP-Exigence SECU_REV_001

Le Titulaire met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent Titulaire en conformité avec les réglementations applicables.

Le Titulaire veille donc à assurer l'ensemble des opérations pour que l'Acheteur puisse reprendre les services dans de bonnes conditions (transfert de compétences, documentations, ...). Durant la phase de réversibilité, l'assurance de la sécurité réside notamment dans :

- La gestion des accès et des habilitations ;
- Le transfert de responsabilités ;
- La fourniture d'informations nécessitant des mesures de protection adaptées ;
- La gestion de la continuité de l'activité.

Le Titulaire reste responsable de la sécurité jusqu'à la fin de la phase de réversibilité.

3.12. Audit de sécurité sur le périmètre du Titulaire

3.12.1. CCAP-Exigence SECU_AUDIT_001

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

3.12.1. CCAP-Exigence SECU_AUDIT_002

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

3.12.1. CCAP-Exigence SECU_AUDIT_003

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

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

3.12.2. CCAP-Exigence SECU_AUDIT_004

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

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

3.12.1. CCAP-Exigence SECU_AUDIT_005

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

3.13. Pénalités

3.13.1. CCAP-Exigence SECU_PEN_001

En complément de l'article 14 du CCAG-TIC, en cas de violation des mesures de sécurité ou de l'obligation de confidentialité, le Titulaire s'expose aux pénalités suivantes :

- En cas de non-respect des règles de sécurité ou de protection des informations sensibles de l'Acheteur n'impliquant pas des données à caractère personnel : application d'une pénalité égale à 5% du montant exécuté HT du marché public à la date de constatation du fait générateur. Cette pénalité passe à 10% dans le cas où l'information est à « Diffusion Restreinte ».
- En cas de non-respect des règles de sécurité ou de protection des informations sensibles de l'Acheteur impliquant des données à caractère personnel : application d'une pénalité égale à 15% du montant exécuté HT du marché public à la date de constatation du fait générateur.

En cas de constatation de plusieurs faits générateurs, les sanctions pécuniaires ainsi établies sont appliquées de façon cumulative. Le montant des pénalités ainsi établies vient en déduction des paiements à effectuer au titre de toute facture afférente aux prestations exécutées à la date de survenance du fait générateur.

Note : Le pourcentage des pénalités doit être défini par l'Acheteur selon le montant du marché et des commandes envisagées.

4. Clauses à intégrer dans le CCTP

Le Cahier des Clauses Techniques Particulières (CCTP) est un document contractuel qui rassemble les clauses techniques d'un marché. L'objet de cette partie est de fournir un ensemble de clauses aux Acheteurs afin de les aider à préciser les exigences de sécurité attendues par l'Acheteur sur les différentes prestations.

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

4.1.1. CCTP-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.

4.1.2. CCTP-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.

4.1.3. CCTP-Exigence SECU_HOM_003

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

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

4.1.4. CCTP-Exigence SECU_HOM_004

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

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

4.1.5. CCTP-Exigence SECU_HOM_005

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

4.1.6. CCTP-Exigence SECU_HOM_006

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

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

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

4.1.7. CCTP-Exigence SECU_HOM_008

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

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

Note :

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

4.1.8. CCTP-Exigence SECU_HOM_009

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

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

4.1.9. CCTP-Exigence SECU_HOM_010

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

4.1.10. CCTP-Exigence SECU_HOM_011

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

4.2. 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.

4.2.1. CCTP-Exigence SECU_MCS_001

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

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

4.2.2. CCTP-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.

4.2.3. CCTP-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.

4.2.4. CCTP-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).

4.2.5. CCTP-Exigence SECU_MCS_005

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

4.2.6. CCTP-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.

4.2.7. CCTP-Exigence SECU_MCS_007

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

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

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

4.2.8. CCTP-Exigence SECU_MCS_008

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

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

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

4.2.9. CCTP-Exigence SECU_MCS_009

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

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

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

4.2.10. CCTP-Exigence SECU_MCS_010

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

4.2.11. CCTP-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.

4.2.12. CCTP-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.

4.2.13. CCTP-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).

4.2.14. CCTP-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.

4.2.15. CCTP-Exigence SECU_MCS_015

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

4.2.16. CCTP-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).

4.2.17. CCTP-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.

4.2.18. CCTP-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.

4.3. Obligations du Titulaire à se conformer à l'Etat de l'art

4.3.1. CCTP-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. Tout

Toutefois, le Titulaire doit respecter les exigences suivantes pour les services Web et de messagerie qu'il serait amené à fournir :

- **Services Web :**
 - o les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, ...) ou une technologie en particulier ;

- o les mécanismes cryptographiques doivent être conformes aux annexes B du référentiel général de sécurité (RGS)¹ de l'ANSSI.
 - o les mécanismes cryptographiques TLS (HTTPS) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications. L'utilisation de la technologie HSTS est fortement recommandée ;
 - o les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
 - o une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;
 - o les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés.
- **Services de messagerie :**
 - o les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, ...) ;
 - o la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (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.

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

4.4.1. CCTP-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.

4.4.2. CCTP-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.

4.4.3. CCTP-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.

4.4.4. CCTP-Exigence SECU_GDB_004

Toute transmission de fichiers sur un support physique (DAT, CDROM, ...), par courrier externe ou par porteur, donne lieu à un accusé de réception. Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'Acheteur. De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

- L'émetteur et le destinataire ;

¹ <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/>

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

4.4.5.CCTP-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.

4.4.6.CCTP-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.

4.4.7.CCTP-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.

4.4.8.CCTP-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.

4.4.9.CCTP-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.

4.5. Obligations du Titulaire sur la sécurité de ses locaux informatiques

4.5.1.CCTP-Exigence SECU_LOC_001

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

4.5.2. CCTP-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.

4.5.3. CCTP-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.

4.5.4. CCTP-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.

4.5.5. CCTP-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.

4.5.6. CCTP-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.

4.5.7. CCTP-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, ...).

4.5.8. CCTP-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.

4.5.9. CCTP-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.

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

4.6.1. CCTP-Exigence SECU_SRE_001

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

4.6.2. CCTP-Exigence SECU_SRE_002

Le Titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration permettant l'accès aux environnements de l'Acheteur depuis le site du Titulaire doivent respecter les exigences suivantes (en suivant, à défaut d'une précision de l'Acheteur, les recommandations de l'ANSSI) :

- Les correctifs de sécurité et les mises à jour antivirus doivent se faire quotidiennement ;
- Tous les outils présents sur le poste doivent être référencés dans le CCT du ministère de l'Intérieur. Toute dérogation doit être expressément validée par le CSN de l'Acheteur ;
- Les postes ne doivent pas avoir accès à internet et à un système d'information bureautique (messagerie, intranet, ...) ;
- Les postes d'administration utilisés doivent être réservés exclusivement à cet usage. Tout accès au poste doit se faire de manière sécurisée que ce soit pour l'ouverture d'une session et l'accès physique ;
- Les postes d'administration doivent être mis sur un VLAN dédié.

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

4.6.3. CCTP-Exigence SECU_SRE_003

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

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

4.6.4. CCTP-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.

4.6.5. CCTP-Exigence SECU_SRE_005

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

4.6.6. CCTP-Exigence SECU_SRE_007

Le Titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

4.6.7. CCTP-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.

4.6.8. CCTP-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.

4.6.9. CCTP-Exigence SECU_SRE_010

Le Titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

4.6.10. CCTP-Exigence SECU_SRE_011

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

4.6.11. CCTP-Exigence SECU_SRE_012

Le Titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège. Attaques en essai et erreurs sur secrets d'authentification : les moyens d'authentification mis en place par le Titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

4.6.12. CCTP-Exigence SECU_SRE_013

Le Titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves. Le Titulaire collecte et stocke à minima les informations suivantes :

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

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

4.6.13. CCTP-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.

4.6.14. CCTP-Exigence SECU_SRE_016

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

4.6.15. CCTP-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.

4.6.16. CCTP-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.

4.6.17. CCTP-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.

4.6.18. CCTP-Exigence SECU_SRE_020

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

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

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

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

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

4.7.1. CCTP-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.

4.7.2. CCTP-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.

4.7.3. CCTP-Exigence SECU_SPT_003

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

4.7.4. CCTP-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.

4.7.5. CCTP-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.

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

4.8.1. CCTP-Exigence SECU_INC_001

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

4.8.2. CCTP-Exigence SECU_INC_002

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

4.8.3. CCTP-Exigence SECU_INC_003

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

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

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

4.8.4. CCTP-Exigence SECU_INC_004

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

4.8.5. CCTP-Exigence SECU_INC_005

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

4.9. Obligations du Titulaire lors de l'accès aux locaux de l'Acheteur

4.9.1. CCTP-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.

4.9.2. CCTP-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.

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

4.10.1. CCTP-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, ...).

4.10.2. CCTP-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.

4.10.3. CCTP-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, ...).

4.10.4. CCTP-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.

4.10.1. CCTP-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.

4.11. 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.

4.11.1. CCTP-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.

4.11.2. CCTP-Exigence SECU_NOMADE_002

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

4.11.3. CCTP-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.

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

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

4.12.1. CCTP-Exigence SECU_INTERCO_001

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

4.12.2. CCTP-Exigence SECU_INTERCO_002

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

4.12.3. CCTP-Exigence SECU_INTERCO_003

En cas d'interconnexion des SI de l'Acheteur et du Titulaire, le Titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI.

L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'Acheteur au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'Acheteur.

4.12.4. CCTP-Exigence SECU_INTERCO_004

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

- Les flux et protocoles autorisés, ainsi que les ressources auxquelles le Titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ;
- Les modalités d'authentification requises : authentification par mot de passe, authentification forte par mot de passe unique ou par certificat ;
- Les modalités de chiffrement des échanges : le chiffrement des flux transitant sur Internet est requis ;
- Les exigences spécifiques de traçabilité des accès ;

- Les moyens de sécurité supplémentaires à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif...

4.13. 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.

4.13.1. CCTP-Exigence SECU_CPE_001

Le Titulaire doit respecter les standards et les méthodologies préconisés au sein de l'Acheteur. En particulier, le Titulaire doit appliquer les méthodes d'évaluation de la sensibilité et d'analyse de risques des systèmes d'information lorsqu'il intervient dans les phases amont des projets.

4.13.2. CCTP-Exigence SECU_CPE_002

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

4.13.3. CCTP-Exigence SECU_CPE_003

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

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

4.14. Obligations du Titulaire sur la sécurité des développements

4.14.1. CCTP-Exigence SECU_DEV_001

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

4.14.2. CCTP-Exigence SECU_DEV_002

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

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

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

- Les entrées des utilisateurs doivent être contrôlées et filtrées (longueur, type de donnée attendue, ...) avant traitement.
- Les contrôles de sécurité sur les entrées et les sorties d'une application doivent être réalisés à minima du côté du composant serveur de l'application.
- Seules les données correspondant à des paramètres attendus doivent être prises en compte.

- o 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).

4.14.3. CCTP-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.

4.14.4. CCTP-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.

4.14.5. CCTP-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.

4.14.6. CCTP-Exigence e SECU_DEV_006

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

4.14.7. CCTP-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, ...).

4.14.8. CCTP-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.

4.14.9. CCTP-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.

4.14.10. CCTP-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.

4.14.11. CCTP-Exigence e SECU_DEV_011

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

4.14.12. CCTP-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.

4.14.13. CCTP-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.

4.14.14. CCTP-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.

4.14.15. CCTP-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.

4.14.16. CCTP-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.

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

4.15.1. CCTP-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.

4.15.2. CCTP-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.

4.15.3. CCTP-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.

4.15.4. 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 amenés, dans le cadre du marché, à mettre en œuvre pour ses propres besoins ou concevoir pour les besoins de l'Acheteur. Si le produit final vise une qualification après la notification du marché, il est fortement recommandé que le jalon J0 du processus de qualification soit franchi préalablement.

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

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

4.15.5. CCAP-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, ...).

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

4.16.1. CCTP-Exigence SECU_ACCES_001

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

4.16.2. CCTP-Exigence SECU_ACCES_002

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

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

4.16.3. CCTP-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.

4.16.4. CCTP-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.

4.17. Obligations du Titulaire dans la gestion des personnels

4.17.1. CCTP-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.

4.17.2. CCTP-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.

4.17.3. CCTP-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.

4.17.4. CCTP-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.

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

4.18.1. CCTP-Exigence SECU_PCA_001

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

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

4.18.2. CCTP-Exigence SECU_PCA_002

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

4.18.3. CCTP-Exigence SECU_PCA_003

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

5. Annexes

5.1. Glossaire

ACHETEUR PUBLIC

Personne qui définit ou met en œuvre des stratégies achat de toute nature en vue de satisfaire les besoins qualitatifs et quantitatifs des services et de contribuer à la performance des achats dans le respect des règles de la commande publique. L'Acheteur public est chargé de piloter les projets achat et de suivre leur exécution, de mesurer la performance achat, de mener la veille économique, notamment en analysant les marchés fournisseurs. Il cherche à promouvoir les marchés disponibles auprès des utilisateurs et mesure leur degré de satisfaction. Il coordonne, en liaison avec les prescripteurs et les approvisionneurs-achat, la définition du juste besoin. Lorsqu'il est chargé de porter la procédure juridique de contractualisation, il rédige les éléments du dossier de consultation relatifs à l'expression du besoin et du choix du fournisseur, analyse les offres, négocie (lorsque cela est permis par la réglementation) et sélectionne les offres attributaires.

APPLICATION

Une application est un ensemble de logiciels nécessaires pour l'exécution d'une tâche donnée.

ATTRIBUTAIRE

L'attributaire d'un marché public est le soumissionnaire classé premier à l'issue de l'analyse des offres auquel il est envisagé d'attribuer le marché.

ACTE D'ENGAGEMENT (AE)

Document contractuel, signé des deux parties qui constitue la pièce principale du marché.

CAHIER DES CHARGES

Document contractuel qui décrit le besoin de l'Acheteur, exprimé sous forme de spécifications techniques et /ou d'exigences fonctionnelles. Il détermine également les conditions dans lesquelles les prestations qui font l'objet du marché doivent être exécutées.

CAHIER DES CLAUSES ADMINISTRATIVES GÉNÉRALES (CCAG)

Arrêté ministériel auquel l'Acheteur peut faire référence dans les documents de la consultation, auquel cas il devient un document contractuel. L'Acheteur a toujours la possibilité d'y déroger de manière expresse au sein des autres pièces contractuelles. Il contient des stipulations d'ordre administratif et financier applicables à un même secteur d'activité. Il existe cinq CCAG en fonction de l'objet du marché :

- Travaux
- Marchés industriels
- Prestations intellectuelles
- Fournitures courantes et prestations de services
- Techniques de l'information et de la communication.

CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIÈRES (CCAP)

Document contractuel qui décrit les conditions administratives particulières d'exécution des marchés, notamment les conditions administratives et financières (avances, acomptes, conditions de livraison, pénalités...).

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

Document contractuel qui décrit les conditions techniques particulières d'exécution des marchés, sous forme d'exigences minimales (approche fonctionnelle) ou de spécifications fonctionnelles techniques.

CADRE DE RÉPONSE

Document que l'Acheteur peut inclure aux documents de la consultation et visant à faciliter l'analyse des offres.

CANDIDAT

Personne physique ou morale publique ou privée qui présente sa candidature dans le cadre d'une procédure de marché public. Dans ce présent guide, la notion de candidat renvoie indifféremment aux notions de candidat au sens strict, mais aussi de soumissionnaire, d'opérateur économique ou d'entreprise.

CANDIDATURE

Document déposé par un candidat à une procédure de marché public relatif notamment à ses aptitudes et capacités pour exécuter le marché public.

DOCUMENTS DE LA CONSULTATION (DC)

L'ensemble des documents fournis par l'Acheteur ou auxquels il se réfère afin de définir ses besoins et de décrire les modalités de la procédure de passation, y compris l'avis d'appel à la concurrence. Les informations fournies sont suffisamment précises pour permettre aux opérateurs économiques de déterminer la nature et l'étendue du besoin et de décider de participer à la procédure.

LOGICIEL

Le logiciel est une œuvre constituée d'un ensemble de programmes, procédés et règles, relatifs au fonctionnement d'un ensemble de traitement de données et la documentation afférente. Le terme logiciel employé seul dans le présent document désigne indifféremment des logiciels standards ou des logiciels spécifiques.

Le logiciel standard est un logiciel conçu par le Titulaire ou un éditeur tiers, pour être fourni à plusieurs utilisateurs en vue de l'exécution d'une même fonction ;

Le logiciel spécifique est un logiciel spécialement développé par le Titulaire pour apporter une solution sur mesure aux besoins propres de l'Acheteur. Il peut s'agir d'une œuvre originale créée ex nihilo, ou de l'adaptation, au moyen de développements spécifiques, d'œuvres préexistantes (logiciels standards ou logiciels spécifiques).

OPÉRATEUR ÉCONOMIQUE

Terme générique qui couvre à la fois les notions d'entrepreneur, fournisseur et prestataire de services. Il désigne toute personne physique ou morale, publique ou privée, ou groupement de ces personnes qui propose une offre dans le cadre d'un marché public pour la réalisation de travaux et/ou d'ouvrages, la fourniture de produits ou de services. Dans ce guide, la notion d'opérateur économique est remplacée par le terme générique de candidat.

PRODUIT

Ensemble des matériels et logiciels d'un éditeur ou fournisseur tiers, acquis par le Titulaire au profit de l'Acheteur.

PRESCRIPTEUR

Personne qui définit techniquement les besoins objet du marché, pour son compte ou celui d'autres personnes. Il est souvent placé dans une direction métier.

PRESTATION

Une prestation désigne les fournitures ou les services, notamment informatiques ou de télécommunication, qui font l'objet du marché.

RÈGLEMENT DE LA CONSULTATION (RC)

Document non contractuel figurant dans les documents de la consultation. Il précise les modalités de la mise en concurrence, les critères d'attribution des offres et leur pondération ainsi que la possibilité d'une négociation. Il complète l'avis d'appel à la concurrence.

RESULTATS (Propriété intellectuelle)

Désignent tous les éléments, quels qu'en soient la forme, la nature et le support, qui résultent de l'exécution des prestations objet du marché, tels que, notamment, les œuvres, les logiciels, leurs mises à jour ou leurs

nouvelles versions, les bases de données, les signes distinctifs, les noms de domaine, les informations, les sites internet, les rapports, les études, les marques, les dessins ou modèles, les inventions brevetables ou non au sens du code de la propriété intellectuelle, et plus généralement tous les éléments protégés ou non par des droits de propriété intellectuelle ou par tout autre mode de protection, tels que le savoir-faire, le secret des affaires, le droit à l'image des biens ou des personnes.

SOUS-TRAITANCE

Opération par laquelle le Titulaire confie, sous sa responsabilité et sous son contrôle, à une autre personne physique ou morale appelée sous-traitant l'exécution d'une partie des tâches qui sont à sa charge dans le cadre du marché public qui lui a été attribué. Le Titulaire demeure, face à la personne publique, le seul responsable de l'exécution des prestations.

TITULAIRE

Le Titulaire est l'opérateur économique qui conclut le marché avec l'Acheteur. En cas de groupement d'opérateurs économiques, le « Titulaire » désigne le groupement représenté par son mandataire. L'attributaire d'un marché public devient le Titulaire de ce marché après qu'il ait apporté la preuve de la régularité de sa situation et suite à la signature du marché et sa notification par l'Acheteur.

SOUSSIONNAIRE

Opérateur économique qui présente une offre dans le cadre d'une procédure de marché public. Dans présent guide le vocable utilisé pour désigner le soumissionnaire est « le candidat ».

5.2. Attestation de reconnaissance de responsabilité (2 pages)



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

ATTESTATION DE RECONNAISSANCE DE RESPONSABILITE

Relative au bon respect des obligations de confidentialité, de protection des données à caractère personnel ou sensibles et des mesures de sécurité en vigueur au ministère de l'intérieur

L'accès aux installations et l'utilisation des ressources informatiques de l'Acheteur doit se faire dans le strict respect de la législation et, en particulier, celle applicable au respect des personnes et de la propriété intellectuelle ainsi qu'aux actes de fraude, de détournement et de malveillance informatique.

Société ____ :

Nom ____ :

Prénom ____ :

Fonction ____ :

Je soussigné(e) reconnais avoir été sensibilisé par le Titulaire responsable de l'exécution du marché et de ce fait m'engage pleinement à :

- Respecter l'obligation de discrétion professionnelle pour tous les faits, informations ou documents dont j'aurais connaissance dans l'exercice ou à l'occasion de l'exercice de mes activités ;
- Prendre connaissance, suivre et respecter les dispositions relatives à la protection et à la confidentialité des informations de l'Acheteur ;
- Ne divulguer, ou ne communiquer à un tiers, en aucun cas des informations ou données tant personnelles que professionnelles que je pourrais être amené(e) à apprendre dans l'exercice de ma mission ;
- Ne pas reproduire, stocker, copier, diffuser, modifier, altérer ou détruire toute information ou donnée dont je pourrais avoir connaissance à d'autres fins que celles de l'exercice de ma mission ;
- Respecter le principe fondamental du « besoin d'en connaître » et ainsi de ne pas tenter d'accéder, de reproduire, de stocker, de copier, de diffuser, de modifier, d'altérer ou de détruire toute information dont je ne suis pas supposé avoir connaissance dans l'exercice de ma mission.

Si, à l'occasion de l'exécution du marché, je dispose d'un accès à un système d'information de l'administration et, par conséquent, d'un compte nominatif, je m'engage également à :

- Ne pas tenter d'introduire et de connecter tout appareil électronique communicant ou non, personnel ou de la société, au système d'information sans avoir reçu préalablement l'autorisation formelle de la voie fonctionnelle SSI ;
- Ne pas modifier sans autorisation la configuration des moyens mis à ma disposition et notamment de ne pas raccorder de moyens informatiques qui n'auront pas été convenus au préalable avec le ministère de l'Intérieur dans le cadre de la définition de l'architecture ;
- Ne pas me livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des services, applications et moyens auxquels j'ai accès ;
- Ne pas mettre à la disposition d'utilisateurs non autorisés un accès privilégié aux ressources informatiques, données ou services ;
- Ne pas perturber ou interrompre le fonctionnement normal du système d'information ou de l'un de ses composants ;
- Ne pas installer, sans autorisation préalable et formelle de la voie fonctionnelle SSI (ou de son représentant) de logiciels sur le système d'information ou sur les équipements mis à ma disposition ;

- Ne pas introduire, tester ou utiliser des supports informatique ou médias dont l'origine m'est inconnue, douteuse ou incertaine ;
- Ne pas générer volontairement ou involontairement des perturbations sur les ressources du SI que ce soit par des manipulations anormales ou par l'introduction illicite de logiciels contrefaits ou piratés potentiellement nuisibles en terme de failles de sécurité ou de pollution virale.

Je déclare être pleinement conscient(e) de mes responsabilités et reconnais être informé(e) des conséquences pénales, et contractuelles qui pourraient résulter de la non application des procédures et dispositions édictées ci-dessus.

Date :

Signature de l'intéressé(e)

Date :

Signature d'une personne physique ayant qualité pour engager la personne morale du Titulaire du marché de prestation et cachet de la société.

EXTRAITS DES ARTICLES RELATIFS AUX DISPOSITIONS GÉNÉRALES RELATIVES À LA FRAUDE INFORMATIQUE

Art. 323-1 du nouveau code pénal : l'accès frauduleux à un système de traitement automatisé de données est sanctionné. Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende.

Art. 323-2 : l'atteinte en disponibilité d'un système de traitement automatisé de données est sanctionnée. Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Art. 323-3 : l'atteinte en intégrité d'un système de traitement automatisé de données est sanctionnée. Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, ou de supprimer ou de modifier frauduleusement des données qu'il contient, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Art. 323-3-1 : l'utilisation, sans motif légitime, d'outils permettant de porter atteinte à un système de traitement automatisé de données est sanctionnée. Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

DISPOSITIONS CONCERNANT LA PROPRIÉTÉ INTELLECTUELLE

Art. L.111-1 du code de la propriété intellectuelle : l'auteur est Titulaire des droits sur les logiciels qu'il crée. L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Toute utilisation faite sans son consentement est considérée comme illicite et sanctionnée pénalement. La seule exception : le droit de courte citation qui permet de reproduire partiellement l'œuvre à condition d'en indiquer clairement l'auteur et la source.

Art. L.112-1&2 du code de la propriété intellectuelle : les logiciels sont protégés par les droits d'auteur. Sont protégées toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, et notamment les logiciels. La mise sur le réseau informatique d'un document doit donc être conditionnée au fait d'être Titulaire des droits sur ce document, ou pour le moins d'être autorisé à le reproduire sur le réseau.

Note : La licence d'un logiciel définit les droits accordés pour son utilisation. En règle générale, une copie de sauvegarde est autorisée.

5.3. Identification des exigences applicables à l'objet du marché

Les tableaux ci-dessous indiquent les types de clauses relevant en fonction de l'objet du marché :

5.3.1. Cas du RC

Objet du Marché →	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
Exigences de sécurité ↓							
Plan d'assurance sécurité							
RC-Exigence SECU_PAS_001	☒	☒	☒	☒	☒	☒	☒
RC-Exigence SECU_PAS_002	☒	☒	☒	☒	☒	☒	☒
RC-Exigence SECU_PAS_003	☒	☒	☒	☒	☒	☒	☒
RC-Exigence SECU_PAS_004	☒	☒	☒	☒	☒	☒	☒
RC-Exigence SECU_PAS_005	☒	☒	☒	☒	☒	☒	
RC-Exigence SECU_PAS_006	☒	☒	☒	☒	☒	☒	☒
Engagement de reconnaissance de responsabilité							
RC-Exigence SECU_ERR_001	☒	☒	☒	☒	☒	☒	☒
Sous-traitance							
RC-Exigence SECU_ST_001	☒	☒	☒	☒	☒		☒
Hébergement							
RC-Exigence SECU_HEB_001	☒	☒	☒	☒	☒		☒
RC-Exigence SECU_HEB_002	☒	☒	☒	☒	☒		☒
RC-Exigence SECU_HEB_003	☒	☒	☒	☒	☒		☒
RC-Exigence SECU_HEB_004				☒			☒
RC-Exigence SECU_HEB_005	☒	☒	☒	☒	☒		☒

5.3.2. Cas du CCAP

Objet du Marché →	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
Exigences de sécurité ↓							
Conformité à l'état de l'art							
CCAP-Exigence SECU_CEA_001	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_CEA_002	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_CEA_003	☒	☒	☒	☒	☒		☒
Cartographie des SI							
CCAP-Exigence SECU_CARTO_001	☒	☒	☒	☒	☒	☒	☒
Protection de l'information							
CCAP-Exigence SECU_PDI_001	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_PDI_002	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_PDI_003	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_PDI_004	☒	☒	☒	☒	☒	☒	☒
Maintien en condition de sécurité							
CCAP-Exigence SECU_MCS_001	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_MCS_002	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_MCS_003	☒	☒	☒	☒	☒		☒
Événements et incidents de sécurité							
CCAP-Exigence SECU_EIS_001	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_EIS_002	☒	☒	☒	☒	☒	☒	☒
Gestion du personnel							
CCAP-EXIGENCE SECU_GDP_001	☒	☒	☒	☒	☒	☒	☒

Objet du Marché →							
Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCAP-EXIGENCE SECU_GDP_002	☒	☒	☒	☒	☒	☒	☒
CCAP-EXIGENCE SECU_GDP_003	☒	☒	☒	☒	☒	☒	☒
CCAP-EXIGENCE SECU_GDP_004	☒	☒	☒	☒	☒	☒	☒
CCAP-EXIGENCE SECU_GDP_005	☒	☒	☒	☒	☒	☒	☒
CCAP-EXIGENCE SECU_GDP_006	☒	☒	☒	☒	☒	☒	☒
CCAP-EXIGENCE SECU_GDP_007	☒	☒	☒	☒	☒	☒	☒
Sécurisation des locaux du titulaire							
CCAP-Exigence SECU_LOC_001	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_LOC_002	☒	☒	☒	☒	☒	☒	☒
Propriété intellectuelle des résultats							
CCAP-Exigence SECU_PI_001	☒	☒	☒	☒	☒	☒	☒
Echéance ou résiliation du marché							
CCAP-Exigence SECU_ERM_001	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_ERM_002	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_ERM_003	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_ERM_004	☒	☒	☒	☒	☒		☒
CCAP-Exigence SECU_ERM_005	☒	☒	☒	☒	☒		☒
Réversibilité							
CCAP-Exigence SECU_REV_001	☒	☒	☒	☒	☒	☒	☒
Audit de sécurité sur le périmètre du Titulaire							

Objet du Marché →							
Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCAP-Exigence SECU_AUDIT_001	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_AUDIT_002	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_AUDIT_003	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_AUDIT_004	☒	☒	☒	☒	☒	☒	☒
CCAP-Exigence SECU_AUDIT_005	☒	☒	☒	☒	☒		☒
Pénalités							
CCAP-Exigence SECU_PEN_001	☒	☒	☒	☒	☒	☒	☒

5.3.3. Cas du CCTP

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
Homologation des SI							
CCTP-Exigence SECU_HOM_001		☒	☒	☒	☒		☒
CCTP-Exigence SECU_HOM_002		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_003		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_004		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_005		☒	☒	☒	☒		☒
CCTP-Exigence SECU_HOM_006		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_007		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_008		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_009		☒	☒	☒	☒		☒
CCTP-Exigence SECU_HOM_010		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_011		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_HOM_012		☒	☒	☒	☒		☒
Maintien en condition de sécurité							
CCTP-Exigence SECU_MCS_001		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_002		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_003		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_004		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_005		☒	☒	☒	☒		☒

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_MCS_006		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_007		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_008		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_009		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_010		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_MCS_011		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_MCS_012		☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_MCS_013		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_014		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_015		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_016		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_017		☒	☒	☒	☒		☒
CCTP-Exigence SECU_MCS_018		☒	☒	☒	☒		☒
Etat de l'art							
CCTP-Exigence SECU_EDA_001		☒	☒	☒	☒		☒
Gestion des biens de l'acheteur							
CCTP-Exigence SECU_GDB_001			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_002			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_003			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_004			☒	☒	☒	☒	☒

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_GDB_005			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_006			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_007			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_008			☒	☒	☒	☒	☒
CCTP-Exigence SECU_GDB_009			☒	☒	☒	☒	☒
Sécurisation des locaux du titulaire							
CCTP-Exigence SECU_LOC_001	☒	☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_LOC_002		☒	☒	☒	☒		☒
CCTP-Exigence SECU_LOC_003	☒		☒	☒	☒		☒
CCTP-Exigence SECU_LOC_004	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_LOC_005	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_LOC_006	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_LOC_007	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_LOC_008	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_LOC_009	☒	☒	☒	☒	☒		☒
Sécurité des réseaux et de l'exploitation							
CCTP-Exigence SECU_SRE_001		☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_002		☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_003		☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_004	☒	☒	☒	☒	☒		☒

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_SRE_005	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_006	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_007	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_008	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_009	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_010	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_011	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_012	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_013	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_014	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_015	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_016	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_017	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_018	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_019	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_SRE_020	☒	☒	☒	☒	☒		☒
Sécurité des postes de travail							
CCTP-Exigence SECU_SPT_001			☒	☒	☒		☒
CCTP-Exigence SECU_SPT_002			☒	☒	☒		☒

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_SPT_003			☒	☒	☒		☒
CCTP-Exigence SECU_SPT_004			☒	☒	☒		☒
CCTP-Exigence SECU_SPT_005			☒	☒	☒		☒
Traitement des incidents de sécurité							
CCTP-Exigence SECU_INC_001		☒		☒		☒	☒
CCTP-Exigence SECU_INC_002		☒		☒		☒	☒
CCTP-Exigence SECU_INC_003		☒		☒		☒	☒
CCTP-Exigence SECU_INC_004		☒		☒		☒	☒
CCTP-Exigence SECU_INC_005		☒		☒		☒	☒
Obligations du Titulaire lors de l'accès aux locaux de l'Acheteur							
CCTP-Exigence SECU_AL_001	☒			☒	☒	☒	☒
CCTP-Exigence SECU_AL_002	☒			☒	☒	☒	☒
Obligations du Titulaire intervenant au sein des locaux de l'Acheteur							
CCTP-Exigence SECU_TIERS_001	☒		☒	☒	☒	☒	☒
CCTP-Exigence SECU_TIERS_002	☒		☒	☒	☒	☒	☒
CCTP-Exigence SECU_TIERS_003	☒		☒	☒	☒	☒	☒
CCTP-Exigence SECU_TIERS_004	☒		☒	☒	☒	☒	☒
CCTP-Exigence SECU_TIERS_005	☒		☒	☒	☒	☒	☒
Nomadisme numérique							
CCTP-Exigence SECU_NOMADE_001	☒	☒	☒	☒	☒		☒

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_NOMADE_002	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_NOMADE_003	☒	☒	☒	☒	☒		☒
Interconnexion avec les SI du Titulaire							
CCTP-Exigence SECU_INTERCO_001	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_INTERCO_002	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_INTERCO_003	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_INTERCO_004	☒	☒	☒	☒	☒		☒
Prestations d'Etude							
CCTP-Exigence SECU_CPE_001	☒		☒	☒	☒	☒	☒
CCTP-Exigence SECU_CPE_002	☒		☒	☒	☒	☒	☒
CCTP-Exigence SECU_CPE_003	☒		☒	☒	☒	☒	☒
Sécurité des développements							
CCTP-Exigence SECU_DEV_001	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_002	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_003	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_004	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_005	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_006	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_007	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_008	☒			☒	☒		☒

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_DEV_009	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_010	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_011	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_012	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_013	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_014	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_015	☒			☒	☒		☒
CCTP-Exigence SECU_DEV_016	☒			☒	☒		☒
Achats de services, matériels ou logiciels							
CCTP-Exigence SECU_AML_001	☒		☒	☒	☒		☒
CCTP-Exigence SECU_AML_002	☒		☒	☒	☒		☒
CCTP-Exigence SECU_AML_003	☒		☒	☒	☒		☒
CCTP-Exigence SECU_AML_004	☒		☒	☒	☒		☒
CCTP-Exigence SECU_AML_005	☒		☒	☒	☒		☒
Gestion des droits d'accès							
CCTP-Exigence SECU_ACCES_001	☒	☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_ACCES_002	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_ACCES_003	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_ACCES_004		☒	☒	☒	☒		☒
Gestion des personnels							

Objet du Marché → Exigences de sécurité ↓	Prestations intellectuelles	Hébergement externalisé	Achats de matériels ou logiciels	Exploitation et supervision	Etudes et développements	MOA	MOE
CCTP-Exigence SECU_PERS_001	☒	☒	☒	☒	☒		☒
CCTP-Exigence SECU_PERS_002	☒	☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_PERS_003	☒	☒	☒	☒	☒	☒	☒
CCTP-Exigence SECU_PERS_004	☒	☒	☒	☒	☒	☒	☒
Plan de continuité d'activité							
CCTP-Exigence SECU_PCA_001		☒		☒	☒	☒	☒
CCTP-Exigence SECU_PCA_002		☒		☒	☒	☒	☒
CCTP-Exigence SECU_PCA_003		☒		☒	☒	☒	☒