

Exigences de sécurité fonctionnelles

Marché AMOE 2027 Annexe CCAP

Version du 14/04/2026

Validée

Classification : Interne

Référence : A définir

Historique et détails des modifications

Version	Crée modifié le	ou	Rédacteur	Nature des mises à jour et commentaires
1.0	20/03/2026		LST/MDE	Initialisation du document
1.1	31/03/2026		LST/MDE	Intégration remarques DAAIS-S
1.2	14/04/2026		LST/MDE	Intégration résultat travail avec DAAIS-S / YPO
1.3	17/04/2026		MDE	Passage en version validée. Suppression des marques et commentaires
1.4	20/04/2026		MDE	Correction coquilles

SOMMAIRE

ARTICLE 0 : OBJET, CHAMP D'APPLICATION ET DEFINITIONS.....	4
0.1 OBJET.....	4
0.2 CHAMP D'APPLICATION.....	4
0.3 DEFINITIONS	4
0.4 NIVEAUX DE CRITICITE.....	4
0.5 HIERARCHIE DES NORMES ET ARTICULATION CONTRACTUELLE	5
0.6 CONVENTION DE LECTURE	5
0.7 PRINCIPE DE PROPORTIONNALITE	5
ARTICLE 1 : PLAN D'ASSURANCE SECURITE	5
ARTICLE 2 : MODALITES APPLICABLES AUX GROUPEMENTS	5
2.1 IDENTIFICATION ET PERIMETRE DE CHAQUE MEMBRE.....	5
2.2 MODALITES DE REPONSE AUX EXIGENCES DE SECURITE	5
2.3 APPLICATION UNIFORME ET EVOLUTIONS DU GROUPEMENT.....	5
2.4 CONTINUITE D'ACTIVITE EN CAS DE DEFAILLANCE D'UN MEMBRE.....	6
ARTICLE 3 : EXIGENCES APPLICABLES AUX FREELANCES ET SALARIES PORTES.....	6
3.1 PRINCIPE DE PORTAGE DES OBLIGATIONS DE SECURITE.....	6
3.2 EXIGENCES POUR TOUT INTERVENANT FREELANCE OU PORTE	6
3.3 REGIME DE RESPONSABILITE	6
ARTICLE 4 : POLITIQUE, ORGANISATION ET GOUVERNANCE.....	6
4.1 DESIGNATION DES INTERLOCUTEURS SECURITE	6
4.2 POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION	7
4.3 CONFORMITE CONTINUE A LA PSSI.....	7
4.4 REFERENT SECURITE ET ATTRIBUTION DES RESPONSABILITES.....	7
4.5 DELAIS DE NOTIFICATION ET DE CORRECTION DES PROBLEMES DE SECURITE.....	7
4.6 PROCESSUS DE SECURITE OBLIGATOIRES.....	7
4.7 DECLARATION ET EVALUATION DE LA SECURITE DES SOUS-TRAITANTS.....	7
ARTICLE 5 : CONFORMITE A L'ETAT DE L'ART ET EXIGENCES TRANSVERSES	8
5.1 CONFORMITE GENERALE	8
5.2 GESTION DES VULNERABILITES ET DES CORRECTIFS.....	8
5.3 GESTION DE L'OBSOLESCENCE TECHNOLOGIQUE	8
5.4 EXIGENCES CRYPTOGRAPHIQUES	8
5.5 SECURITE DES RESEAUX ET DES COMMUNICATIONS.....	8
ARTICLE 6 : GESTION DE PROJETS.....	8
6.1 INTEGRATION DE LA SECURITE DANS LE CYCLE DE VIE	8
6.2 REFERENT SECURITE PROJET	9
6.3 ANALYSE DE RISQUES SECURITE	9
ARTICLE 7 : SECURITE DES DEVELOPPEMENTS.....	9
7.1 CHAINE DE DEVELOPPEMENT SECURISE	9
7.2 DOCUMENTATION TECHNIQUE DE SECURITE	9
7.3 REFERENTIELS DE DEVELOPPEMENT SECURISE.....	9
7.4 CORRECTION DES VULNERABILITES	10
7.5 SEPARATION DES ENVIRONNEMENTS PROTECTION DES DONNEES DE TEST	10
7.6 TRAÇABILITE, INTEGRITE ET SECURITE DU CODE SOURCE.....	10
7.7 TESTS D'INTRUSION AVANT MISE EN PRODUCTION.....	10
ARTICLE 8 : RESSOURCES HUMAINES ET CONTROLE D'ACCES.....	10
8.1 CONFORMITE ET ADHESION AUX DOCUMENTS NORMATIFS DE L'ACOSS.....	10
8.2 POSTE DE TRAVAIL MAITRISE ET SECURISE	10
8.3 GESTION DU CYCLE DE VIE DES INTERVENANTS	11
8.4 FORMATION INITIALE A LA SECURITE	11
8.5 SENSIBILISATION CONTINUE.....	11
8.6 FORMATION AU DEVELOPPEMENT SECURISE.....	11
8.7 FORMATION A L'INTEGRATION DE LA SECURITE DANS LES PROJETS.....	11
8.8 AUTHENTIFICATION ET CONTROLE D'ACCES LOGIQUE	11
8.9 CONDITIONS D'ACCES AU SYSTEME D'INFORMATION DE L'ACOSS ET GESTION DES LICENCES	12

8.10 GESTION DES ACCES A PRIVILEGES	12
ARTICLE 9 : GESTION DES BIENS ET DES DONNEES	12
9.1 IDENTIFICATION, CLASSIFICATION ET ISOLATION DES DONNEES	12
9.2 TRAÇABILITE ET PROTECTION DES DONNEES	12
9.3 SUPPORTS AMOVIBLES ET TRANSFERTS DE DONNEES	13
9.4 RESTITUTION ET DESTRUCTION DES DONNEES EN FIN DE MARCHE	13
9.5 INVENTAIRE DES ACTIFS	13
ARTICLE 10 : CONFIDENTIALITE	13
10.1 DEFINITION ET PERIMETRE DES INFORMATIONS CONFIDENTIELLES	13
10.2 OBLIGATIONS DE PROTECTION	13
10.3 DUREE ET SURVIE DE L'OBLIGATION	14
ARTICLE 11 : TRAITEMENT DES INCIDENTS DE SECURITE CONCERNANT DES DONNEES OU DES SYSTEMES DE L'ACOSS	14
11.1 OBLIGATION DE NOTIFICATION ET DELAIS	14
11.2 PROCEDURES DE REPONSE, TRAÇABILITE ET REPORTING	14
11.3 PLAN DE GESTION DE CRISE INFORMATIQUE	14
11.4 DETECTION, PRESERVATION DES PREUVES ET COOPERATION FORENSIQUE	14
11.5 ASTREINTE SECURITE ET RETOUR D'EXPERIENCE	14
11.6 COMMUNICATION LIEE A L'INCIDENT	15
ARTICLE 12 : CONTINUITE D'ACTIVITE ET SAUVEGARDES	15
12.1 PLAN DE CONTINUITE ET PLAN DE REPRISE D'ACTIVITE	15
12.2 TESTS, EXERCICES ET RESILIENCE CYBER	15
12.3 PROCEDURE D'ACTIVATION	15
ARTICLE 13 : LIEU D'EXECUTION ET HEBERGEMENT	15
13.1 DECLARATION ET SECURITE DES LIEUX D'EXECUTION	15
13.2 EXECUTION DES PRESTATIONS HORS DE FRANCE	15
13.3 HEBERGEMENT DES DONNEES ET LOIS EXTRATERRITORIALES	16
13.4 SECURITE PHYSIQUE DES INFRASTRUCTURES D'HEBERGEMENT	16
ARTICLE 14 : UTILISATION DE L'INTELLIGENCE ARTIFICIELLE	16
14.1 INTERDICTION PAR DEFAULT	16
14.2 OBLIGATIONS DE TRANSPARENCE ET DE QUALITE	16
14.3 SANCTIONS EN CAS DE MANQUEMENT	16
ARTICLE 15 : AUDIT DE SECURITE	16
15.1 DROIT D'AUDIT PERMANENT	16
15.2 MODALITES DE REALISATION DES AUDITS	16
15.3 TESTS D'INTRUSION ET CHARTE D'AUDIT	16
15.4 PLAN D'ACTIONS CORRECTIVES	16
ARTICLE 16 : PROTECTION DES DONNEES A CARACTERE PERSONNEL	17
16.1 QUALIFICATION ET ENCADREMENT DU TRAITEMENT	17

Article 0 : Objet, champ d'application et définitions

0.1 Objet

La présente annexe définit les exigences de sécurité fonctionnelles et de protection des données personnelles applicables au marché public de prestations informatiques. Elle constitue une pièce contractuelle du marché, annexée au Cahier des Clauses Administratives Particulières (CCAP).

0.2 Champ d'application

Les exigences de la présente annexe s'appliquent à l'ensemble des lots du marché, à tous les bons de commande émis dans le cadre de l'accord-cadre, et à l'intégralité des prestations exécutées au titre du marché, y compris celles exécutées par des sous-traitants, des membres du groupement, des freelances ou des salariés portés.

0.3 Définitions

Les termes définis ci-dessous sont employés avec une majuscule initiale dans le corps du document.

Terme	Définition
Pouvoir adjudicateur / Acooss	L'Acooss, agissant en qualité de pouvoir adjudicateur au sens du code de la commande publique, y compris ses représentants habilités. Les deux termes sont utilisés de manière interchangeable et désignent la même entité.
Titulaire	L'opérateur économique attributaire du marché, agissant seul ou dans le cadre d'un groupement.
Entité de rattachement sécurité	Personne morale expressément désignée dans le Plan d'Assurance Sécurité (PAS) pour garantir et assumer, vis-à-vis de l'Acooss, l'entière responsabilité du respect des exigences de la présente annexe par un Intervenant qui n'est pas son salarié direct (notamment un freelance ou un salarié porté), au même titre que s'il l'était.
Intervenant	Toute personne physique exécutant des prestations au titre du marché, quel que soit son statut (salarié du Titulaire, salarié d'un sous-traitant, freelance, salarié porté, intérimaire).
Données de l'Acooss	Toute donnée, sous quelque forme et sur quelque support que ce soit, dont l'Acooss est propriétaire, détentrice ou responsable de traitement, et qui est communiquée au Titulaire, produite et traitée pour le compte de l'Acooss ou accessible par le Titulaire dans le cadre du marché. Cela inclut les données à caractère personnel, les données métier, les codes source, la documentation, les configurations et les secrets.
Données confidentielles	Sous-ensemble des Données de l'Acooss dont la compromission aurait un impact significatif. Cela incluent a minima : les données à caractère personnel de toute catégorie, les données couvertes par le secret des affaires, les données financières non publiques, les secrets cryptographiques, les données d'authentification et les codes source. En cas de doute, la donnée est réputée confidentielle. Les données confidentielles sont plus largement détaillées à l'Article 10.
Incident de sécurité	Tout événement indésirable ou inattendu présentant une probabilité significative de compromettre la confidentialité, l'intégrité, la disponibilité des Données de l'Acooss ou des systèmes d'information utilisés dans le cadre du marché, y compris celui du pouvoir adjudicateur. Cela inclut les violations de données à caractère personnel au sens de l'article 4.12 du RGPD.
Problème de sécurité	Toute non-conformité aux exigences de la présente annexe, toute vulnérabilité technique exploitable ou tout défaut de configuration susceptible de conduire à un Incident de sécurité.
Poste de travail maîtrisé	Poste de travail dont le Titulaire ou l'Entité de rattachement sécurité assure l'administration, la configuration, la mise à jour, la supervision de sécurité et le contrôle d'accès, et qui satisfait aux critères de l'article EX-SEC-RH-02.
Mesure conservatoire	Action technique ou organisationnelle d'urgence mise en œuvre pour contenir un risque immédiat, sans nécessairement constituer la correction définitive.
Sinistre majeur	Événement entraînant une indisponibilité prolongée (supérieure à quatre heures) des moyens nécessaires à l'exécution des prestations, ou une compromission affectant significativement les Données de l'Acooss.
Évolution significative	Modification d'un système ou d'un périmètre altérant l'architecture de sécurité, les flux de données, les mécanismes d'authentification, l'exposition réseau ou le périmètre des données traitées.
Évolution majeure	Évolution significative dont l'impact sur la surface d'attaque justifie une nouvelle analyse de risques ou un nouveau test d'intrusion. En cas de désaccord sur la qualification, celle de l'Acooss prévaut.
CVSS	Common Vulnerability Scoring System, version 3.1 ou version ultérieure la plus récente publiée par le FIRST. En cas de divergence entre sources, le score le plus élevé est retenu.
Jours ouvrés	Du lundi au vendredi, hors jours fériés au sens du code du travail français.
Heures ouvrées	De 7 h 00 à 19 h 00 en jours ouvrés.

0.4 Niveaux de criticité

La présente annexe repose sur une échelle unique de criticité applicable aux Incidents de sécurité, aux Problèmes de sécurité et aux vulnérabilités techniques :

Niveau	Définition
Critique	Compromission active, exfiltration de données, indisponibilité majeure, violation de données à caractère personnel, vulnérabilité avec exploit actif ou CVSS ≥ 9.0.
Élevé	Impact significatif sur la confidentialité, l'intégrité ou la disponibilité ; CVSS compris entre 7.0 et 8.9 inclus.
Modéré	Impact limité sur la sécurité de l'information ; CVSS compris entre 4.0 et 6.9 inclus.
Faible	Impact mineur sur la sécurité de l'information ; CVSS inférieur à 4.0.

La criticité est évaluée conjointement par le Titulaire et l'Acoss. En cas de désaccord, l'évaluation de l'Acoss prévaut. L'Acoss peut réévaluer la criticité à la hausse à tout moment en justifiant cette réévaluation.

0.5 Hiérarchie des normes et articulation contractuelle

En cas de contradiction entre la présente annexe et d'autres pièces contractuelles, l'ordre de priorité est celui défini à l'article 4 du CCAP. En cas de contradiction entre la présente annexe et la PSSI du Titulaire, la présente annexe prévaut.

0.6 Convention de lecture

Les exigences préfixées **EX-SEC** sont obligatoires. Les exigences préfixées **SO-SEC** sont souhaitées et valorisées lors de l'analyse des offres. Le verbe « doit » exprime une obligation ; « il est souhaité » exprime une recommandation.

0.7 Principe de proportionnalité

Lorsqu'une exigence prévoit un dispositif organisationnel ou un outil spécifique, le Titulaire peut, s'il ne dispose pas d'une structure dédiée en raison de sa taille, démontrer dans le PAS qu'il atteint un niveau de protection équivalent par des moyens alternatifs proportionnés, notamment le recours à un prestataire externe identifié dans le PAS ou l'utilisation de services managés. Le pouvoir adjudicateur apprécie si les moyens alternatifs offrent un niveau de protection équivalent. L'invocation de la taille du Titulaire ne peut en aucun cas justifier l'absence totale de mise en œuvre d'une exigence obligatoire.

Article 1 : Plan d'Assurance Sécurité

EX-SEC-PAS-01

Le Titulaire élabore, met en œuvre, maintient à jour et fait respecter, par lui-même et par ses éventuels sous-traitants, un Plan d'Assurance Sécurité **spécifiquement conçu pour répondre à chaque exigence** du présent document pendant toute la durée du marché et dénommé PAS dans la suite du document. Ce PAS initial est remis dans le cadre de la réponse technique. Le Titulaire fournit également dans le cadre de la réponse technique son organisation en matière de protection des données personnelles. Ces dispositions peuvent être contenues dans le PAS ou dans un document spécifique à part.

Article 2 : Modalités applicables aux groupements

Lorsque la candidature est présentée par un groupement d'opérateurs économiques, le PAS doit satisfaire, outre l'article 1, aux exigences suivantes.

2.1 Identification et périmètre de chaque membre

EX-SEC-GRP-01

Le PAS identifie de façon explicite le type de groupement, chaque membre du groupement, précise son rôle et son périmètre d'intervention, et désigne le mandataire comme interlocuteur unique du pouvoir adjudicateur pour toutes les questions relatives à la sécurité de l'information. Le PAS doit préciser les certifications de chaque membre du groupement.

2.2 Modalités de réponse aux exigences de sécurité

EX-SEC-GRP-02

Pour chaque exigence de la présente annexe :

- si la réponse est commune à l'ensemble des membres, elle peut être formulée une seule fois au nom du groupement, sous réserve de le mentionner explicitement ;
- si la réponse diffère selon les membres, une réponse individualisée par membre est exigée, en identifiant clairement le membre concerné.

Toute réponse ne permettant pas de déterminer sans ambiguïté la répartition des rôles et des responsabilités entre les membres est considérée comme non conforme.

2.3 Application uniforme et évolutions du groupement

EX-SEC-GRP-03

Les exigences de sécurité s'appliquent à chacun des membres pour son périmètre d'intervention, sans exception ni atténuation, sauf dérogation expressément acceptée par le pouvoir adjudicateur. Toute modification de la composition ou de l'organisation du groupement est notifiée au pouvoir adjudicateur dans un délai maximal de cinq (5) jours ouvrés, ou dans les vingt-quatre (24) heures si la modification résulte d'une défaillance ou d'un incident de sécurité. Un PAS mis à jour est fourni sous dix (10) jours ouvrés.

2.4 Continuité d'activité en cas de défaillance d'un membre

EX-SEC-GRP-04

Le PCA du groupement couvre les scénarios de défaillance temporaire ou définitive d'un membre, y compris une société de portage ou une plateforme de freelances, et prévoit :

- les mesures de prise en charge transitoire par le mandataire ou un autre membre ;
- un plan de substitution en cas de défaillance prolongée, incluant la reprise du périmètre par les membres restants ou un tiers approuvé par le pouvoir adjudicateur.

En cas de groupement solidaire, chaque membre s'engage à prendre en charge les activités de tout autre membre défaillant dans les limites de ses compétences techniques.

Article 3 : Exigences applicables aux freelances et salariés portés

Le présent article s'applique à tout Intervenant freelance, salarié porté ou mis à disposition par une société de portage ou une plateforme d'intermédiation, en complément de l'ensemble des autres articles.

3.1 Principe de portage des obligations de sécurité

EX-SEC-FREE-01

Le pouvoir adjudicateur n'accepte aucune situation dans laquelle un Intervenant ne serait couvert par aucune Entité de rattachement sécurité.

- Pour chaque freelance ou salarié porté, un membre identifié du groupement ou le Titulaire lui-même est désigné comme « **Entité de rattachement sécurité** » et assume la totalité des obligations de sécurité comme s'il s'agissait de son propre salarié.
- La société de portage ne peut être Entité de rattachement sécurité que si elle démontre disposer des moyens organisationnels et techniques effectifs (PSSI, gestion des postes, sensibilisation, gestion des incidents). À défaut, c'est le membre du groupement disposant du système de management de la sécurité qui porte ces obligations.

3.2 Exigences pour tout Intervenant freelance ou porté

EX-SEC-FREE-02

L'Entité de rattachement sécurité s'assure de l'application stricte des exigences du présent document aux freelances, en veillant tout particulièrement aux règles concernant tous les Intervenants :

- Article 8 : Ressources humaines et contrôle d'accès
- Article 10 : Confidentialité
- Article 14 : Utilisation de l'intelligence artificielle

EX-SEC-FREE-03

L'Entité de rattachement sécurité formalise et s'assure que chaque freelance dispose d'une procédure de notification des incidents avec un point de contact identifié au sein de l'Entité de rattachement sécurité, laquelle est responsable de la notification au pouvoir adjudicateur dans les délais de l'article 11. Le freelance préserve les preuves et coopère en cas d'investigation.

3.3 Régime de responsabilité

EX-SEC-FREE-04

L'Entité de rattachement sécurité assume, vis-à-vis du pouvoir adjudicateur, une obligation de résultat quant au respect des exigences de sécurité pour chaque Intervenant freelance ou porté qui lui est rattaché.

En cas de groupement solidaire, chaque membre est tenu solidairement de l'ensemble des obligations de sécurité, y compris celles relatives aux Intervenants rattachés à un autre membre.

Aucune entité ne peut s'exonérer en invoquant le statut d'indépendant du freelance ou l'absence de lien de subordination.

Article 4 : Politique, organisation et gouvernance

4.1 Désignation des interlocuteurs sécurité

EX-SEC-GOUV-01

Dès la notification de l'accord-cadre, le Titulaire désigne nommément et communique au pouvoir adjudicateur les coordonnées de contact des interlocuteurs suivants :

- le responsable de l'accord-cadre ;
- le responsable de la sécurité des systèmes d'information (RSSI), disposant d'un niveau d'autorité suffisant pour prendre des décisions opérationnelles et engager les ressources en cas d'incident ;
- le délégué à la protection des données (DPO).

Pour chaque rôle, un suppléant est identifié. Tout changement est notifié par écrit cinq (5) jours ouvrés avant sa prise d'effet, sauf force majeure où la notification intervient dans les vingt-quatre (24) heures.

4.2 Politique de sécurité des systèmes d'information

EX-SEC-GOUV-02

Le Titulaire dispose d'une PSSI complète, documentée, approuvée par sa direction, dont la dernière revue date de moins de vingt-quatre (24) mois. Un résumé exécutif est transmis dans le cadre du PAS. Le pouvoir adjudicateur peut consulter la PSSI complète à tout moment et sur simple demande. En cas d'écart entre la PSSI et les exigences du marché, les exigences du marché prévalent.

4.3 Conformité continue à la PSSI

EX-SEC-GOUV-03

Le Titulaire est effectivement conforme à sa PSSI durant toute la durée du marché. Cette conformité est démontrable sur demande par la production d'éléments probants (audits internes ou externes, certifications, registre des non-conformités). En cas de perte d'une certification ou de non-conformité majeure, le Titulaire en informe le pouvoir adjudicateur par écrit sous cinq (5) jours ouvrés et propose un plan de remédiation sous dix (10) jours ouvrés.

4.4 Référent sécurité et attribution des responsabilités

EX-SEC-GOUV-04

Le Titulaire dispose d'un référent sécurité en charge de l'application opérationnelle de la PSSI, ayant autorité pour imposer les exigences de sécurité du présent document à l'ensemble des Intervenants. La PSSI attribue explicitement les fonctions et responsabilités liées à la sécurité. Le PAS présente un organigramme fonctionnel de la sécurité identifiant les rôles et la chaîne d'escalade.

4.5 Délais de notification et de correction des Problèmes de sécurité

EX-SEC-GOUV-05

Le Titulaire identifie, notifie et corrige tout Problème de sécurité, tels que les non-conformités aux exigences de ce document ou tout défaut de configuration susceptible de conduire à un Incident de sécurité, dans les délais suivants, calculés à compter de la détection ou de la notification, selon l'événement survenant en premier. Les vulnérabilités logicielles (soumises à publication de patch) relèvent de l'article 5.2 :

Niveau	Délai de notification	Mesure conservatoire	Correction définitive
Critique	12 h	Immédiate (4 h max.)	3 jours ouvrés
Élevé	12 h ouvrées	Sous 24 h	15 jours ouvrés
Modéré	5 jours ouvrés	NC	3 mois
Faible	Reporting périodique	NC	12 mois

Tout Problème de criticité Critique ou Elevé fait l'objet d'un rapport de clôture incluant l'analyse des causes, les mesures correctives et les actions préventives. Le pouvoir adjudicateur peut refuser la clôture du problème si la correction est jugée insuffisante.

La notification d'un Problème de criticité Critique ou Elevé et le rapport de clôture associé sont envoyés aux personnes concernées avec en copie le RSSI National de l'Acoss. Lorsque le problème implique des données à caractère personnel, la DPO de l'Acoss est informée simultanément.

4.6 Processus de sécurité obligatoires

EX-SEC-GOUV-06

Le Titulaire définit, documente et met en œuvre effectivement les processus suivants dans sa PSSI:

- gestion et réponse aux Incidents de sécurité ;
- gestion des correctifs de sécurité ;
- surveillance et gestion des vulnérabilités ;
- gestion de la sécurité des fournisseurs et sous-traitants ;
- analyse et gestion des risques selon une méthodologie formalisée ;
- sensibilisation et formation à la sécurité (programme annuel documenté) ;
- gestion de la continuité d'activité ;
- gestion des actifs et classification de l'information.

Le Titulaire décrit dans le PAS de manière synthétique chacun des processus.

SO-SEC-GOUV-01

Il est souhaité que le Titulaire dispose d'une certification ISO/IEC 27001 en cours de validité couvrant le périmètre des activités réalisées pour l'Acoss. Dans le cadre d'un groupement, chaque membre précise et fournit les certifications dont il est titulaire.

SO-SEC-GOUV-02

Il est souhaité que le Titulaire dispose d'un SOC interne ou externalisé assurant une surveillance en 24/7 des environnements nécessaire à la réalisation des prestations du marché.

4.7 Déclaration et évaluation de la sécurité des sous-traitants

EX-SEC-GOUV-07

Préalablement à toute intervention d'un sous-traitant, et au plus tard lors de la transmission du formulaire de déclaration de sous-traitance (DC4), le Titulaire fournit obligatoirement au pouvoir adjudicateur le résultat d'une autoévaluation formalisée du niveau de couverture des exigences de la présente annexe par le sous-traitant pressenti.

Cette autoévaluation doit démontrer que le sous-traitant a mis en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité au moins équivalent à celui exigé du Titulaire, sur le périmètre des prestations qui lui est confié.

Le pouvoir adjudicateur se réserve le droit de refuser l'acceptation du sous-traitant si les garanties de sécurité présentées dans cette autoévaluation sont jugées insuffisantes, incomplètes, ou non conformes aux exigences du marché. Ce refus, dûment motivé par des critères de sécurité de l'information, ne donne lieu à aucune indemnité pour le Titulaire.

Article 5 : Conformité à l'état de l'art et exigences transverses

5.1 Conformité générale

EX-SEC-EA-01

Le Titulaire maintient un niveau de sécurité conforme à l'état de l'art, aux bonnes pratiques (guides de l'ANSSI, recommandation de la CNIL, normes ISO/IEC 27001 et 27002) et à la législation en vigueur (RGPD, le cas échéant NIS 2 et règlement 2024/1689 AI Act). Ils mettent en œuvre des mesures techniques et organisationnelles appropriées pour assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données et des systèmes. Le Titulaire fournit sur demande les preuves de conformité (certifications, rapports d'audit, attestation signée par le RSSI).

5.2 Gestion des vulnérabilités et des correctifs

EX-SEC-EA-02

Le Titulaire met en œuvre un processus de veille en vulnérabilités et de gestion des correctifs couvrant l'ensemble des composants techniques du marché notamment les systèmes et applications qui hébergent et traitent ou contribuent au traitement des données de l'Acoss. Les correctifs sont appliqués dans les délais suivants pour les environnements en production :

Niveau	CVSS	Mesure conservatoire	Délai d'application
Critique	≥ 9.0 ou exploit actif	Immédiate (4h max)	3 jours ouvrés
Élevé	$7.0 \leq CVSS < 9.0$	Sous 24h	15 jours ouvrés

En cas d'impossibilité d'appliquer un correctif dans les délais, le Titulaire met en œuvre des mesures compensatoires documentées, en informe le pouvoir adjudicateur sous quarante-huit (48) heures et fournit un plan de remédiation. Le Titulaire notifie le pouvoir adjudicateur sous douze (12) heures pour toute vulnérabilité critique exploitable affectant les systèmes ou données de l'Acoss.

5.3 Gestion de l'obsolescence technologique

EX-SEC-EA-03

Sauf à ce que le pouvoir adjudicateur soit responsable de l'obsolescence des composants à utiliser, pour des contraintes qui lui sont propres, le Titulaire n'utilise pas de composants en situation d'obsolescence de sécurité (ne faisant plus l'objet de correctifs). En cas d'impossibilité de remplacement à court terme, le Titulaire notifie le pouvoir adjudicateur par écrit sous dix (10) jours ouvrés (sous quarante-huit (48) heures si le composant est exposé sur Internet ou traite des Données confidentielles), produit une analyse de risques, met en œuvre des mesures compensatoires et propose un plan de migration. L'utilisation sans notification préalable et sans mesures compensatoires constitue un manquement.

5.4 Exigences cryptographiques

EX-SEC-EA-04

Le Titulaire met en œuvre des mécanismes cryptographiques à l'état de l'art, conformes au RGS et aux recommandations de l'ANSSI en vigueur.

5.5 Sécurité des réseaux et des communications

EX-SEC-EA-05

Le Titulaire met en oeuvre une organisation de sécurité réseau garantissant a minima :

- l'isolement des environnements de l'Acoss des autres environnements du Titulaire ;
- l'autorisation des seuls flux de communication strictement nécessaires, formalisés et revus au moins une fois par an ;
- une protection renforcée des systèmes exposés sur Internet manipulant des données de l'Acoss ;
- la sécurisation et le chiffrement de tous les accès à distance ;
- une surveillance des flux réseau permettant de détecter les comportements anormaux.

Le Plan d'Assurance Sécurité (PAS) décrit l'architecture réseau sous forme de schéma indiquant les zones de confiance, les points de contrôle et les flux autorisés.

Article 6 : Gestion de projets

6.1 Intégration de la sécurité dans le cycle de vie

EX-SEC-PROJ-01

Les méthodes de gestion de projets utilisées pour l'Acoss intègrent la sécurité à chaque étape (conception, développement, recette,

déploiement, exploitation, maintien en condition opérationnelle, décommissionnement). Les principes de Privacy by Design et Security by Default sont appliqués systématiquement, quel que soit le projet.

6.2 Référent sécurité projet

EX-SEC-PROJ-02

Pour chaque projet significatif (plus de 500 jh ou concernant un Système d'Information Essentiel), le Titulaire désigne un référent sécurité projet nommément identifié. Ce référent sécurité apportera son expertise aux équipes projets du Titulaire durant les différentes étapes du cycle de vie des projets et sera l'interlocuteur privilégié de l'ACOSS pour les aspects de sécurité du projet. Ce référent est l'interlocuteur du pouvoir adjudicateur pour la sécurité du projet, il veille à l'exécution des jalons de sécurité et formule un avis sécurité lors de chaque décision de mise en production. La désignation intervient au lancement du projet. Tout changement est notifié sous cinq (5) jours ouvrés.

6.3 Analyse de risques sécurité

EX-SEC-PROJ-03

Pour tout projet impliquant le traitement de Données confidentielles, la conception d'une nouvelle architecture ou l'exposition de services sur Internet, le pouvoir adjudicateur peut décider de mener une analyse de risques selon la méthodologie EBIOS Risk Manager à laquelle le Titulaire contribue en fonction de son niveau de responsabilité dans le projet. L'analyse couvre les actifs, les données traitées, les flux et les interfaces avec les systèmes de l'Acoss. Elle est transmise au pouvoir adjudicateur pour validation et mise à jour à chaque Évolution significative. Le pouvoir adjudicateur peut exiger la prise en compte de scénarios supplémentaires, demander des mesures complémentaires ou refuser la poursuite du projet si le risque résiduel est jugé inacceptable.

Si une analyse d'impact sur la vie privée (AIPD – article 35 du RGPD) est nécessaire, le Titulaire s'engage à apporter assistance dans la conduite de l'analyse à la DPO de l'ACOSS et son équipe.

Article 7 : Sécurité des développements

7.1 Chaîne de développement sécurisé

EX-SEC-DEV-01

Le Titulaire met en œuvre une chaîne de développement sécurisé intégrant au minimum :

- des outils d'analyse statique de code ;
- des outils d'analyse dynamique ;
- des outils d'analyse de composition logicielle ;
- des outils de détection de secrets dans le code source et les fichiers de configuration ;
- des tests de sécurité automatisés couvrant les fonctions de sécurité.

Le résultat des tests de sécurité listés ci-dessus font partie des livrables obligatoires à fournir au pouvoir adjudicateur.

Le PAS précise les outils utilisés, leur périmètre et leur fréquence d'exécution. Le Titulaire produit sur demande un inventaire complet des composants logiciels incluant les vulnérabilités connues et le statut de support. Le pouvoir adjudicateur peut demander l'utilisation d'outils complémentaires ou procéder à ses propres analyses en complément.

7.2 Documentation technique de sécurité

EX-SEC-DEV-02

Le Titulaire produit ou contribue en fonction de son niveau de responsabilité dans le développement, et maintient à jour, les livrables nécessaires et notamment une documentation technique de sécurité couvrant a minima :

- les mécanismes d'authentification et de gestion des sessions ;
- la gestion des droits et habilitations selon le principe du moindre privilège ;
- les méthodes de stockage sécurisé et de protection des Données confidentielles ;
- les algorithmes et protocoles de chiffrement utilisés ;
- la journalisation des événements de sécurité ;
- les mécanismes de validation des entrées et les protections contre les attaques ;
- la matrice des flux réseaux entre les différents composants ;
- une cartographie des flux de données en cas de transfert de données hors de l'Union Européenne ou vers un tiers.

Cette documentation est transmise avant la mise en production. La mise en production est conditionnée à sa validation formelle par le pouvoir adjudicateur et à l'absence de vulnérabilité d'un niveau Critique ou Elevé non corrigée.

7.3 Référentiels de développement sécurisé

EX-SEC-DEV-03

Le Titulaire met en œuvre les référentiels de bonnes pratiques de développement sécurisé tels que l'OWASP Top 10, l'OWASP ASVS et les recommandations de l'ANSSI applicables. Il se conforme aux exigences spécifiques de l'Acoss en matière de développement sécurisé qui lui sont communiquées. A ce titre, l'Acoss, dispose d'un catalogue en constante évolution d'Exigences Fonctionnelles et Non Fonctionnelles à intégrer dans les projets, en fonction des cas d'usages. En cas de contradiction, les exigences de l'Acoss prévalent.

7.4 Correction des vulnérabilités

EX-SEC-DEV-04

Le Titulaire corrige, au titre de la garantie et dans les délais de la PSSI du pouvoir adjudicateur, toute vulnérabilité introduite par les opérations de développement réalisées par le Titulaire, qu'elle soit signalée par le pouvoir adjudicateur, découverte par le Titulaire ou identifiée par un tiers. Il recherche et corrige systématiquement toutes les occurrences de la même erreur dans l'ensemble du code sous sa responsabilité. Pour toute vulnérabilité de niveau Critique ou Elevé, il réalise une analyse des causes racines et propose des mesures préventives.

Délais définis de la PSSI-MCS de l'Acos :

Niveau	CVSS	Mesure conservatoire	Délai d'application
Critique	≥ 9.0 ou exploit actif	Immédiate (4h max)	3 jours ouvrés
Élevé	$7.0 \leq CVSS < 9.0$	Sous 24h	15 jours ouvrés
Modéré	$4.0 \leq CVSS < 7.0$		3 mois
Faible	< 4.0		12 mois

7.5 Séparation des environnements protection des données de test

EX-SEC-DEV-05

Le Titulaire maintient et travaille dans le cadre d'une séparation stricte entre les environnements de développement, de test, de pré-production et de production. Les accès à chaque environnement sont distincts et contrôlés indépendamment. Aucun déploiement direct depuis un environnement de développement vers la production n'est autorisé.

EX-SEC-DEV-06

Le Titulaire s'engage à n'utiliser, dans les environnements de test ou de développement, soit des jeux de données synthétiques dont il a la responsabilité, soit des jeux de données fournis par le pouvoir adjudicateur. Dans ce cas, ceux-ci doivent être anonymisés ou à minima pseudonymisés par le pouvoir adjudicateur. Si le Titulaire utilise des jeux de données non fictifs et non anonymisés, il s'engage à respecter toutes les obligations du RGPD sur la protection des données personnelles et à signaler le problème conformément à l'exigence EX-SEC-GOUV-05 du présent document.

7.6 Traçabilité, intégrité et sécurité du code source

EX-SEC-DEV-07

Tout code source développé pour le compte de l'Acos dans l'environnement du Titulaire est hébergé dans un système de gestion de versions offrant un historique complet et une traçabilité nominative des modifications. Les dépôts sont protégés par un contrôle d'accès strict, distincts des dépôts d'autres clients, et soumis à une revue régulière des droits d'accès. Il est interdit de stocker du code source de l'Acos sur un dépôt personnel ou public, un support amovible non chiffré, ou de le transmettre par un canal non sécurisé. Dans le cadre de développement dans l'environnement de l'Acos, le Titulaire utilise le système de gestion de versions mis à la disposition par le pouvoir adjudicateur.

7.7 Tests d'intrusion avant mise en production

EX-SEC-DEV-08

Pour tout développement d'une application de criticité élevée (application exposée sur Internet, application traitant des Données confidentielles en masse, application ayant un impact métier critique), un test d'intrusion avant la première mise en production et après toute Évolution majeure doit être réalisé. Ce test d'intrusion est assuré par l'Acos. Si l'hébergement de l'application est sous la responsabilité du Titulaire ou d'un sous-traitant, le Titulaire s'engage à ce que le pouvoir adjudicateur puisse réaliser ce test d'intrusion. La mise en production est conditionnée à l'absence de vulnérabilité d'un niveau Critique ou Elevé non corrigée et à la validation du pouvoir adjudicateur. Le pouvoir adjudicateur peut réaliser ses propres tests d'intrusion à tout moment.

Article 8 : Ressources humaines et contrôle d'accès

8.1 Conformité et adhésion aux documents normatifs de l'Acos

EX-SEC-RH-01

Le Titulaire s'engage à respecter les documents applicables de l'Acos (charte des utilisateurs du SI, règlement intérieur, règles d'utilisation des ressources informatiques). Ces documents, qui ont valeur contractuelle, sont communiqués lors de la notification de l'accord-cadre et doivent être retournés signés par le Titulaire sous quinze (15) jours ouvrés.

Le Titulaire assure la diffusion effective de ces documents à l'ensemble de ses Intervenants. À ce titre, avant toute prise de fonction et préalablement à tout accès aux systèmes ou aux Données de l'Acos, le Titulaire s'assure que chaque Intervenant a pris connaissance de ces règles (notamment la charte des utilisateurs du SI) et s'engage formellement à les respecter. Le Titulaire doit être en mesure d'en apporter la preuve sur simple demande du pouvoir adjudicateur.

8.2 Poste de travail maîtrisé et sécurisé

EX-SEC-RH-02

Sauf pour certaines activités très spécifiques qui nécessitent un niveau de sécurité fort et pour lesquelles le pouvoir adjudicateur fournit un poste de travail maîtrisé par l'Acos, le Titulaire s'engage à ce que lui-même ainsi que ses sous-traitants éventuels, connectés au SI de l'ACOSS, qu'il soit en télétravail, dans les locaux de l'ESN, ou connecté à distance, dispose d'un poste de travail fourni et maîtrisé par

le Titulaire ou l'Entité de rattachement sécurité et ne se connecte au SI du Titulaire et de l'ACOSS que depuis ce poste de travail maîtrisé. Ce poste maîtrisé est :

- à jour de ses correctifs de sécurité ;
- chiffré intégralement ;
- équipé d'une solution assurant la sécurité globale du poste de travail, supervisée et mise à jour ;
- doté d'un verrouillage automatique après maximum quinze (15) minutes d'inactivité ;
- administré par le Titulaire ou l'Entité de rattachement sécurité.

L'utilisateur ne dispose pas de droits d'administration locale sur ce poste de travail, sauf dérogation justifiée et documentée.

8.3 Gestion du cycle de vie des Intervenants

EX-SEC-RH-03

Le Titulaire fournit l'identité complète de chaque Intervenant au maximum cinq (5) jours ouvrés avant le début de la prestation. Le pouvoir adjudicateur peut refuser l'accès à toute personne ne répondant pas aux exigences de sécurité. Le Titulaire informe l'Acoss de la fin de mission de chaque Intervenant, si possible avant le départ et au plus tard le jour ouvré suivant. Il garantit, avant le départ effectif ou sous quarante-huit (48) heures en cas d'urgence, la restitution des équipements et documents, l'effacement sécurisé des données, la révocation de tous les accès.

Dans le cadre de sa réponse, le Titulaire précise les processus et procédures mises en œuvre pour prendre en charge la création, la modification et la suppression sécurisées de comptes d'utilisateurs dans le système ou les applications.

8.4 Formation initiale à la sécurité

EX-SEC-RH-04

Tout nouvel Intervenant est formé aux règles de sécurité de l'information avant sa prise de fonction. La formation couvre les principes fondamentaux, la confidentialité, la protection des Données confidentielles et des données personnelles, les menaces courantes et la conduite à tenir en cas d'incident. Des modules spécifiques sont prévus pour les rôles sensibles (administrateurs, développeurs, chefs de projet). Le Titulaire conserve une trace (date, contenu, attestation) et la met à disposition sur demande.

8.5 Sensibilisation continue

EX-SEC-RH-05

Le Titulaire met en place un programme de sensibilisation régulier, continu et documenté incluant des campagnes d'information sur les menaces émergentes et des exercices pratiques (simulations d'hameçonnage, d'ingénierie sociale).

8.6 Formation au développement sécurisé

EX-SEC-RH-06

Toute personne impliquée dans la conception, le développement et les tests de logiciels est formée aux bonnes pratiques du développement sécurisé (vulnérabilités courantes, techniques d'attaque, contre-mesures, outils de sécurité, processus de développement sécurisé). Cette formation est renouvelée au maximum tous les trois (3) ans. Le contenu des formations est communiqué au pouvoir adjudicateur sur simple demande.

8.7 Formation à l'intégration de la sécurité dans les projets

EX-SEC-RH-07

Le personnel intervenant en chefferie de projet ou assimilée est formé aux méthodes d'intégration de la sécurité dans les projets (gestion des risques, exigences de sécurité, spécifications, suivi des plans d'actions, validation de conformité). Cette formation est dispensée avant toute prise de fonction sur un projet de l'Acoss et renouvelée au maximum tous les trois (3) ans. Le contenu des formations est communiqué au pouvoir adjudicateur sur simple demande.

8.8 Authentification et contrôle d'accès logique

EX-SEC-RH-08

a) Authentification multifacteur (MFA)

L'authentification multifacteur est obligatoire pour tout accès distant de l'Intervenant au SI du Titulaire.

SO-SEC-RH-01

a) Authentification multifacteur (MFA)

Il est souhaité que le Titulaire impose l'authentification multifacteur pour l'ouverture de session à tous les postes de travail maîtrisés par le Titulaire.

b) Politique de mots de passe

Il est souhaité que le Titulaire s'engage à mettre en œuvre une politique de mot de passe ayant au minimum les caractéristiques équivalentes à la PSSI de l'Acoss avec une longueur de douze (12) caractères pour les comptes utilisateurs, seize (16) caractères pour les comptes à privilèges. Ceux-ci doivent être complexes et utiliser les 4 classes de caractères.

c) Revue des accès

Il est souhaité que le Titulaire procède à une revue des droits d'accès à son SI au moins tous les douze (12) mois et à chaque changement significatif. Les comptes inactifs depuis plus de quatre-vingt-dix (90) jours sont désactivés automatiquement.

Le Titulaire précise dans le PAS les mesures mises en œuvre dans son SI pour l'authentification et le contrôle d'accès logique.

8.9 Conditions d'accès au système d'information de l'Acosse et gestion des licences

EX-SEC-RH-09

Lorsque les prestations nécessitent un accès au système d'information de l'Acosse, les règles suivantes s'appliquent :

a) Gestion des identités et des licences

Sauf disposition contraire précisée dans le CCTP, l'Acosse fournit, administre et gère les comptes nominatifs, les droits d'accès et les licences logicielles nécessaires pour accéder à son propre système d'information. Le Titulaire s'engage à n'utiliser que les comptes et moyens d'accès fournis par l'Acosse pour toute connexion, locale ou à distance, au SI de l'Acosse. L'intervenant s'engage à installer et utiliser sur le système d'information de l'Acosse que les logiciels qui ont été préalablement et explicitement autorisés par le pouvoir adjudicateur.

Par défaut, le Titulaire ou l'Entité de rattachement sécurité attribue une licence Office 365 à chaque intervenant nécessitant un accès au Tenant Office 365 administré par l'Acosse. Exceptionnellement, si la mission confiée à l'intervenant le justifie, l'Acosse fournit une licence Office 365. Cette licence Office 365 ne peut être utilisée que depuis un terminal maîtrisé par le pouvoir adjudicateur.

b) Privilèges sur les postes de travail fournis par l'Acosse

Par défaut, les Intervenant disposent uniquement de droits d'utilisateur standard sur les postes de travail (qu'ils soient physiques ou virtuels) mis à disposition par l'Acosse. L'attribution de droits d'administration locale est par défaut interdite. Une exception peut toutefois être accordée sous réserve d'une demande de dérogation (temporaire ou permanente) dûment justifiée par l'Intervenant et soumise à la validation préalable et formelle du service du RSSI National de l'Acosse.

c) Interdiction des comptes partagés

L'utilisation de comptes partagés ou génériques dans le SI de l'Acosse est strictement interdite, sauf exception justifiée et préalablement approuvée par le pouvoir adjudicateur.

8.10 Gestion des accès à privilèges

EX-SEC-RH-10

Le Titulaire met en œuvre dans son SI un dispositif de gestion des accès à privilèges aux données de l'Acosse incluant :

- l'inventaire exhaustif et à jour des comptes à privilèges ;
- l'attribution nominative de chaque compte (l'utilisation de comptes génériques (root, admin...) pour les opérations courantes doit être interdite) ;
- l'utilisation d'un équipement centralisé de gestion des accès d'administration aux environnements de production et pré-production, assurant l'authentification renforcée, la traçabilité complète des accès et des actions ;
- le changement des mots de passe des comptes à privilèges immédiatement en cas de départ d'un Intervenant en ayant connaissance ;
- le changement des secrets des comptes de service au minimum tous les douze (12) mois ;
- la séparation des comptes : un compte d'administration distinct du compte utilisateur courant.

Le PAS décrit de manière synthétique le dispositif mis en œuvre.

Article 9 : Gestion des biens et des données

9.1 Identification, classification et isolation des données

EX-SEC-GB-01

Les Données de l'Acosse sont formellement identifiées, inventoriées et classifiées selon leur sensibilité dès leur prise en charge. Elles sont isolées de manière logique et, lorsque la sensibilité le justifie, physique, des données d'autres clients ou tiers. Seul le personnel dûment habilité et autorisé peut y accéder, dans le respect du besoin d'en connaître. Toute tentative d'accès non autorisée est journalisée et notifiée.

Tous documents bureautique produits par le Titulaire, à destination du pouvoir adjudicateur, respecte la Politique de classification des données de l'Acosse. Cette politique lui sera communiquée lors de la phase d'initialisation du marché.

9.2 Traçabilité et protection des données

EX-SEC-GB-02

Le Titulaire met en place des mesures permettant de tracer les accès aux Données de l'Acosse, de détecter tout accès suspect et de se protéger contre tout traitement non autorisé, transfert illicite, perte, destruction, altération ou divulgation accidentelle. Pour répondre à ce besoin, les journaux intègre au minimum, les événements suivants :

- authentifications réussies et échouées ;
- élévations de privilèges et changements de droits ;
- accès et opérations sur les Données confidentielles (lecture, écriture, modification, suppression) ;
- actions d'administration système et applicative ;
- modifications de configuration de sécurité ;
- démarrages, arrêts et redémarrages des systèmes critiques.

Chaque enregistrement doit permettre de déterminer de manière fiable qui a réalisé quelle action et à quel moment.

Les journaux sont centralisés, protégés contre toute modification ou suppression, et conservés douze (12) mois. En cas d'incident impactant des données de l'Acoss, ils sont mis à disposition du pouvoir adjudicateur sous cinq (5) jours ouvrés dans un format exploitable.

9.3 Supports amovibles et transferts de données

EX-SEC-GB-03

L'utilisation de supports amovibles pour les Données de l'Acoss est par défaut interdite sauf dérogation dûment justifiée et validée par le pouvoir adjudicateur. Tout transfert de données est légitime, autorisé, réalisé via un canal chiffré et authentifié, et tracé. L'utilisation de services de partage grand public (WeTransfer, Google Drive, Dropbox, etc.) est interdite. Tout transfert hors de l'Union européenne est interdit sauf autorisation écrite préalable du pouvoir adjudicateur et mise en œuvre de garanties conformes au RGPD (notamment la signature des clauses contractuelles types).

Tout transfert de données vers un tiers ou vers une entité se situant hors de l'Union Européenne doit être explicitement tracé.

9.4 Restitution et destruction des données en fin de marché

EX-SEC-GB-04

Au terme du marché ou en cas de résiliation anticipée, le Titulaire restitue au pouvoir adjudicateur une copie intégrale et complète de l'intégralité des données dans un format exploitable. Après acceptation de la restitution, le Titulaire détruit de manière sécurisée et irréversible, sous un (1) mois, toutes les copies (y compris sauvegardes, archives, postes des freelances et sous-traitants). La restitution et la destruction font l'objet d'un procès-verbal daté et signé attestant qu'aucune copie n'est conservée. Les procédés de destruction garantissent l'impossibilité de récupération. Le pouvoir adjudicateur peut vérifier l'effectivité de la destruction.

9.5 Inventaire des actifs

EX-SEC-GB-05

Le Titulaire établit et maintient à jour un inventaire exhaustif des actifs matériels et logiciels utilisés dans le cadre du marché, couvrant : les postes de travail (y compris ceux des freelances), les serveurs et environnements d'hébergement, les équipements mobiles, les logiciels et outils de développement, les services cloud et SaaS, et les supports amovibles. Cet inventaire est communiqué sur demande et sert de base pour la gestion des vulnérabilités, la vérification de l'obsolescence et la réversibilité.

Article 10 : Confidentialité

10.1 Définition et périmètre des informations confidentielles

EX-SEC-CONF-01

Par dérogation à l'article 5.1.2 du CCAG-TIC, constitue une information confidentielle toute information de quelque nature et sous quelque forme que ce soit, dont l'Acoss est propriétaire ou détentrice, communiquée au Titulaire ou obtenue par ce dernier dans le cadre du marché. Le Titulaire et ses Intervenants ne peuvent l'utiliser que pour l'accomplissement des prestations. N'est pas confidentielle toute information dont le Titulaire prouve qu'elle était dans le domaine public, qu'elle a été signalée comme non confidentielle par l'Acoss, ou qu'elle a été légalement communiquée par un tiers autorisé. La charge de la preuve incombe au Titulaire.

Il faut entendre par données, informations et documents confidentielles :

a) Les données à caractère personnel :

Les données à caractère personnel sont entendues telles qu'elles sont définies à l'article 4.1 du RGPD. Les données à caractère personnel sont protégées par le RGPD et la loi Informatique et Libertés.

b) Les données protégées par la loi, à savoir :

- Une donnée dont la divulgation porte atteinte au secret des affaires (lequel protège les informations économiques et financières des entreprises non divulguées par ces dernières) ;
- Une donnée dont la divulgation porte atteinte à la sécurité publique, à la sécurité des personnes ou la sécurité du système d'information ;
- Une donnée dont la divulgation porterait atteinte à la recherche et à la prévention, par les services compétents, d'infractions de toute nature ou porterait atteinte au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ;
- Une donnée dont la divulgation porterait atteinte à la monnaie et au crédit public (c'est-à-dire aux actes et engagements qui naissent de la faculté de contracter une dette publique par l'emprunt) ;
- Un objet de droit de propriété intellectuelle de tiers dont l'utilisation projetée est susceptible de porter atteinte à ce droit.

10.2 Obligations de protection

EX-SEC-CONF-02

Le Titulaire protège les informations confidentielles avec au moins le même niveau de protection que ses propres informations les plus sensibles, et en tout état de cause un niveau raisonnable et proportionné. Il est interdit de stocker des informations confidentielles sur un espace non maîtrisé, les transmettre via un canal non sécurisé, les communiquer à un tiers non autorisé, photographier ou filmer des écrans ou documents sans autorisation, publier des informations relatives au marché sur une plateforme publique. Le Titulaire s'assure avant toute prise de fonction que chaque Intervenants soit informé et s'engage à respecter ces obligations. Le Titulaire est en capacité à démontrer l'information et l'engagement pris par chaque Intervenants.

10.3 Durée et survie de l'obligation

EX-SEC-CONF-03

L'obligation de confidentialité s'applique sans limitation de durée.

Article 11 : Traitement des Incidents de sécurité concernant des données ou des systèmes de l'Acoss

11.1 Obligation de notification et délais

EX-SEC-INC-01

Le Titulaire informe l'Acoss de tout Incident de sécurité concernant les systèmes, les applications ou les données du marché selon les délais suivants :

Niveau	Délai de notification	Canal	Destinataires
Critique	12 heures	Téléphone puis courriel	cos@acoss.fr et 0986000951
Élevé	12 heures ouvrées	Téléphone puis courriel	cos@acoss.fr et 0986000951
Modéré	5 jours ouvrés	Courriel	cos@acoss.fr
Faible	Reporting mensuel	Courriel	cos@acoss.fr

Pour tout incident de niveau Critique ou Elevé, le Titulaire informe simultanément le RSSI National de l'Acoss.

Lorsque l'incident implique une violation de données à caractère personnel tel que défini par l'article 4. 12) du RGPD, la DPO de l'Acoss est alertée simultanément via l'adresse informatiqueetlibertes.acoss@acoss.fr.

11.2 Procédures de réponse, traçabilité et reporting

EX-SEC-INC-02

Le Titulaire dispose d'un plan de réponse aux incidents documenté et opérationnel, couvrant : détection, qualification, confinement, investigation, éradication, remédiation et retour d'expérience. Il conserve un registre des incidents (chronologie, mesures correctives, statut de clôture) pendant toute la durée du marché.

Pour tout incident du niveau Critique ou Elevé, le Titulaire fournit :

- un bulletin d'information, sous quarante-huit (48) heures (nature, périmètre estimé, mesures immédiates) ;
- un rapport final sous quinze (15) jours ouvrés après clôture (chronologie, causes, impact, mesures correctives et préventives).

Un bulletin d'information intermédiaire (avancement de l'investigation, mesures d'endiguement, mesures de remédiation) est communiqué au maximum sous cinq (5) jours ouvrés et autant de fois que nécessaire et au minimum une fois par semaine en fonction de la durée et de l'évolution de l'incident.

Le pouvoir adjudicateur peut refuser la clôture si le rapport ou les mesures sont jugés insuffisants.

11.3 Plan de gestion de crise informatique

EX-SEC-INC-03

Le Titulaire dispose d'un plan de gestion de crise couvrant les incidents majeurs. Ce plan définit :

- la gouvernance de crise ;
- les critères de déclenchement et niveaux d'escalade ;
- les critères de sortie de la crise ;
- les procédures de communication (y compris via des moyens indépendants du SI compromis) ;
- les scénarios couverts ;
- les procédures de continuité et de reprise associées.

Le plan est testé au moins une fois par an et mis à jour après chaque exercice ou incident.

11.4 Détection, préservation des preuves et coopération forensique

EX-SEC-INC-04

Le Titulaire dispose de moyens de détection proportionnés à la sensibilité des données et systèmes. En cas d'incident de niveau Critique ou Elevé, il préserve l'intégrité de l'ensemble des preuves numériques et s'abstient de toute action susceptible de les altérer, sauf nécessité d'endiguement documentée. Les preuves sont conservées au minimum douze (12) mois après clôture. Le Titulaire coopère pleinement avec les équipes d'investigation du pouvoir adjudicateur ou du tiers mandaté.

11.5 Astreinte sécurité et retour d'expérience

EX-SEC-INC-05

Le Titulaire garantit la joignabilité d'un interlocuteur sécurité décisionnaire, pour les incidents de niveau Critique, sous une (1) heure en heures ouvrées et sous deux (2) heures hors heures ouvrées.

Pour les autres criticités d'incidents, sous vingt-quatre (24) heures en jours ouvrés et sous quarante-huit (48) heures en jours non ouvrés.

Le PAS décrit le dispositif d'astreinte, les coordonnées et les moyens alternatifs de communication. Pour tout incident de niveau Critique ou Elevé, un retour d'expérience formel est organisé sous trente (30) jours ouvrés (analyse des causes, évaluation de la réponse, plan d'actions correctives avec responsables et échéances). Il est transmis par écrit et, pour les incidents de niveau Critique, fait l'objet d'une réunion de restitution.

11.6 Communication liée à l'incident

EX-SEC-INC-06

Le Titulaire s'engage à ce que toute information relative à un Incident de sécurité concernant les données de l'Acos, hébergées par le Titulaire ou par le pouvoir adjudicateur, ne soient pas divulguées sans l'approbation expresse du RSSI National de l'Acos, sauf si la loi l'exige.

Article 12 : Continuité d'activité et sauvegardes

12.1 Plan de Continuité et Plan de Reprise d'Activité

EX-SEC-CA-01

Le Titulaire dispose d'un PCA et d'un PRA documentés, approuvés par sa direction, maintenus à jour et adaptés pour répondre et maintenir les services fournis à l'Acos.

Le PCA identifie les activités critiques, les dépendances techniques et humaines, les stratégies de continuité et le niveau minimal de service garanti pendant la crise.

Le PRA décrit les procédures de reconstruction et de reprise dans le respect des objectifs RTO et RPO définis dans les documents du marché. Les environnements de secours sont géographiquement distincts et indépendants sur le plan réseau et sécurité.

Le Titulaire intègre un volet de résilience face aux cyberattaques. Il dispose d'au moins une copie de sauvegarde hors ligne ou technologiquement immuable des données critiques de l'Acos, non accessible en cas de compromission.

12.2 Tests, exercices et résilience cyber

EX-SEC-CA-02

Le PCA et le PRA sont testés au moins une fois par an au moyen d'exercices couvrant des scénarios réalistes, y compris des cyberattaques. Les plans sont mis à jour en fonction des résultats et de l'évolution des services.

Le Titulaire précise dans le PAS les derniers exercices réalisés avec notamment les dates de réalisation et les scénarios.

12.3 Procédure d'activation

EX-SEC-CA-03

En cas d'activation du PCA ou du PRA sur le périmètre des opérations réalisées pour l'Acos dans le cadre de ce marché, le Titulaire notifie le pouvoir adjudicateur sous deux (2) heures, communique un plan de continuité d'activité même en mode dégradé ou de reprise sous vingt-quatre (24) heures et maintient le niveau minimal de service convenu. Aucune mesure de sécurité ne peut être désactivée sans accord écrit préalable du pouvoir adjudicateur.

Le Titulaire ouvre une cellule de crise à laquelle sont invités le RSSI National, le responsable du département sécurité et le porteur de lot de l'Acos.

Article 13 : Lieu d'exécution et hébergement

13.1 Déclaration et sécurité des lieux d'exécution

EX-SEC-LOC-01

Le Titulaire déclare dans le PAS puis à chaque modification l'ensemble des lieux d'exécution. Il tient à jour un registre (adresse, type de local, Intervenants, mesures de sécurité physique). Les locaux offrent des garanties proportionnées : contrôle d'accès, protection contre la consultation des écrans par des tiers, rangements sécurisés. En télétravail, l'Intervenant utilise exclusivement le Poste de travail maîtrisé (EX-SEC-RH-02) et une connexion sécurisée (VPN ou équivalent). La prestation en télétravail se réalise exclusivement depuis un lieu préalablement approuvé par le Titulaire et conforme à l'exigence EX-SEC-LOC-02.

13.2 Exécution des prestations hors de France

EX-SEC-LOC-02

Les prestations sont exécutées en France par défaut. Toute exécution depuis un autre pays de l'UE est soumise à déclaration préalable écrite. Toute exécution depuis un pays tiers est soumise à autorisation écrite préalable et assortie d'un PAS spécifique (mesures renforcées, analyse de risques, et si des données personnelles sont concernées, AIPD et clauses contractuelles types détaillant les mesures de sécurité, la finalité du transfert et les catégories de données concernées).

L'exécution depuis un pays faisant l'objet de sanctions internationales ou de mesures restrictives de l'UE ou de la France est strictement interdite et ne peut faire l'objet d'aucune dérogation. L'exécution depuis un pays identifié par l'Acos comme présentant des risques majeurs de surveillance étatique est interdite, sauf dérogation exceptionnelle écrite et motivée fondée sur une analyse de risques.

L'absence de réponse ne vaut jamais autorisation. L'exécution depuis un lieu non autorisé ou le défaut de déclaration constitue une faute grave.

13.3 Hébergement des données et lois extraterritoriales

EX-SEC-LOC-03

Les Données de l'Acosson sont hébergées exclusivement dans des centres de données situés dans l'Union européenne. Les services cloud utilisés sont déclarés dans le PAS (localisation, fournisseur, certifications). Tout changement de localisation est soumis à approbation écrite préalable.

Le Titulaire déclare son exposition, et celle de ses sous-traitants et hébergeurs, à des législations extraterritoriales sur l'ensemble de la chaîne (fournisseur, société mère, hébergeur, services cloud). Le Titulaire notifie le pouvoir adjudicateur sous vingt-quatre (24) heures en cas de demande d'accès d'une autorité étrangère, sauf interdiction légale, auquel cas il conteste ou limite la demande et informe le pouvoir adjudicateur sous vingt-quatre (24) heures après levée de l'interdiction.

13.4 Sécurité physique des infrastructures d'hébergement

EX-SEC-LOC-04

Les centres de données hébergeant les Données et/ou systèmes de l'Acosson offrent une sécurité physique conforme à l'état de l'art notamment contre les risques d'intrusion par des moyens de détection, des contrôles d'accès physique avec traçabilité, la protection contre les risques environnementaux (incendie, inondation, coupure électrique), et une surveillance permanente. Le Titulaire précise dans le PAS les certifications détenues.

Article 14 : Utilisation de l'intelligence artificielle

14.1 Interdiction par défaut

EX-SEC-IA-01

Le cadre d'utilisation de tout outil ou service d'intelligence artificielle est décrit dans l'article 14 du CCAP. Les dispositions ci-dessous complètent cet article et le cas échéant déroge à cet article. L'article 14 du CCTP vient préciser les modalités d'usage de l'intelligence artificielle et les situations dans lesquelles celle-ci est autorisée pour le présent Marché.

14.2 Obligations de transparence et de qualité

EX-SEC-IA-02

En cas d'usage autorisé, le Titulaire informe le pouvoir adjudicateur de tout livrable produit avec l'assistance d'un outil d'IA, en précisant l'outil et le degré d'intervention. Tout contenu généré ou assisté par IA est revu, validé et approuvé par un Intervenant humain qualifié avant livraison. Le Titulaire demeure responsable de la qualité, de la conformité et de la sécurité de tous les livrables. Il garantit que l'usage d'IA ne porte atteinte à aucun droit de propriété intellectuelle.

14.3 Sanctions en cas de manquement

EX-SEC-IA-03

L'utilisation d'un outil d'IA non autorisé constitue un manquement grave pouvant conduire à la suspension immédiate des accès de l'Intervenant concerné et la possibilité pour le pouvoir adjudicateur de résilier le marché aux torts exclusifs du Titulaire, sans préjudice de dommages et intérêts. Le Titulaire est responsable de tout manquement de ses Intervenants et de ses sous-traitants ultérieurs.

Article 15 : Audit de sécurité

15.1 Droit d'audit permanent

EX-SEC-AUDIT-01

Le pouvoir adjudicateur dispose d'un droit d'audit permanent sur le périmètre du marché, portant sur le respect des exigences de la présente annexe, des clauses de sous-traitance au sens du RGPD et/ou des clauses contractuelles types, la conformité du PAS, le respect des autorisations délivrées par l'ACOSS conformément aux présentes exigences et l'effectivité des mesures. Ce droit s'étend à l'ensemble de la chaîne de sous-traitance. Le Titulaire sécurise contractuellement ce droit d'audit dans ses contrats avec ses sous-traitants et fournisseurs. Le droit est maintenu pendant toute la durée du marché et douze (12) mois après son terme pour les vérifications relatives à la restitution et à la destruction des données.

15.2 Modalités de réalisation des audits

EX-SEC-AUDIT-02

Les audits sont réalisés par le pouvoir adjudicateur ou un tiers qualifié lié par une obligation de confidentialité. Le Titulaire est informé par écrit avec un préavis de quinze (15) jours ouvrés. Le Titulaire apporte une coopération pleine et entière (accès aux locaux, systèmes, documents, journaux et personnes).

15.3 Tests d'intrusion et charte d'audit

EX-SEC-AUDIT-03

Le pouvoir adjudicateur peut réaliser ou faire réaliser des tests d'intrusion sur les systèmes et applications du Titulaire. Ces tests font l'objet d'une charte signée préalablement (périmètre, méthodologie, limites, contacts d'urgence, responsabilités), annexée au PAS.

15.4 Plan d'actions correctives

EX-SEC-AUDIT-04

Le Titulaire met en œuvre, sans surcoût, un plan d'actions correctives pour toute non-conformité ou vulnérabilité constatée lors des audits, dans les délais des articles EX-SEC-EA-02 et EX-SEC-GOUV-05. Le plan priorise les vulnérabilités critiques et désigne un responsable et une échéance par action. Un constat n'est clos qu'après validation formelle par le pouvoir adjudicateur. Les frais d'audit sont à la charge du Titulaire en cas de manquements avérés ; dans le cas contraire, à la charge du pouvoir adjudicateur.

Article 16 : Protection des données à caractère personnel

16.1 Qualification et encadrement du traitement

EX-SEC-DCP-01

Lorsque le Titulaire traite des données à caractère personnel pour le compte de l'Acos, il agit en qualité de sous-traitant au sens de l'article 28 du RGPD. Les conditions sont encadrées par un accord de traitement des données annexé au marché [Annexe CCAP - Sous-traitance de traitement de données à caractère personnel].