

ANNEXE 3 CCAP - EXIGENCES DE SECURITE

Sécurité Informatique

Orientations Générales

ANNEXE 3 CCAP EXIGENCES DE SECURITE

TABLE DES MATIERES

1	INTRODUCTION	1
1.1	Champ d'application	1
1.2	Objectif du document	1
2	EXIGENCES	1
2.1	Plan d'Assurance Sécurité	Erreur ! Signet non défini.
2.2	Politique, organisation, gouvernance	1
2.3	Conformité à l'état de l'art du SI du Titulaire	Erreur ! Signet non défini.
2.4	Gestion de projets	Erreur ! Signet non défini.
2.5	Sécurité des développements	Erreur ! Signet non défini.
2.6	Ressources humaines	1
2.7	Gestion des biens	1
2.8	Obligation de confidentialité	2
2.9	Traitement des incidents	2
2.10	Continuité d'activité	2
2.11	Lieu d'exécution	2
2.12	Utilisation de ressources basées sur l'intelligence artificielle	3
2.13	Audit de sécurité	6

1 INTRODUCTION

1.1 CHAMP D'APPLICATION

Marché public induisant des problématiques de cybersécurité.

1.2 OBJECTIF DU DOCUMENT

L'objectif de ce document est de lister les exigences de sécurité à intégrer dans un marché afin que les prestataires soient en mesure d'apporter un niveau de sécurité satisfaisant face aux attentes de l'ACOSS et aux risques auxquels l'ACOSS est exposé.

2 EXIGENCES

2.1 POLITIQUE, ORGANISATION, GOUVERNANCE

EX-SEC-GOUV-01 : Dès la notification de l'accord cadre, le Titulaire nomme un responsable de l'accord-cadre, lequel sera l'interlocuteur privilégié du pouvoir adjudicateur pour le suivi et l'exécution du contrat.

Le Titulaire désigne aussi :

- Le responsable de la sécurité du système d'information habilité à le représenter auprès de l'ACOSS pour traiter tout problème de sécurité durant toute la durée de l'accord-cadre.
- Le délégué à la protection des données.

2.2 RESSOURCES HUMAINES

EX-SEC-RH-01 : Le Titulaire et ses sous-traitants éventuels sont tenus de respecter strictement les prescriptions et interdictions figurant dans les documents applicables au sein de l'ACOSS. Sont notamment visées les règles s'imposant en matière d'utilisation des ressources informatiques, de communications électroniques et téléphoniques, y compris celles qui concernent les moyens d'accès distants au système d'information de l'ACOSS présents dans la charte des utilisateurs du SI et le règlement intérieur en cas de présence du prestataire dans nos locaux. Les documents applicables au sein de l'ACOSS sont communiqués au Titulaire à la notification de l'accord-cadre puis retournés signés par ce dernier et ont valeur contractuelle.

EX-SEC-RH-02 : Dans le cadre des accès à distance au système d'information de l'ACOSS, le Titulaire s'engage à fournir l'identité de chaque personne devant intervenir avec un délai de prévenance d'au minimum 5 jours ouvrés avant le début de la prestation. De plus le Titulaire s'engage à informer l'ACOSS, si possible avant le départ, et au plus tard le jour ouvré suivant son départ, de la fin de mission de chaque intervenant afin que ses moyens d'accès au SI de l'ACOSS soient désactivés sans délais, puis supprimés. Ces connexions à distance sur le SI de l'ACOSS sont réalisées en utilisant uniquement les moyens techniques fournis par l'ACOSS.

EX-SEC-RH-05 : Le Titulaire doit former tout nouveau personnel aux règles de sécurité de l'information avant leur prise de fonction et avant tout accès aux systèmes ou aux données de l'ACOSS. Cette formation doit couvrir les principes de base de la sécurité, la protection des données sensibles et la conduite à tenir en cas d'incident de sécurité. Des modules spécifiques doivent être prévus pour les rôles sensibles, tels que les administrateurs système, les développeurs et les chefs de projet. Le Titulaire doit conserver une trace de ces formations et la mettre à disposition de l'ACOSS sur demande.

EX-SEC-RH-06 : Le Titulaire doit mettre en place des actions de sensibilisation régulières et variées pour maintenir un haut niveau de vigilance de son personnel face aux menaces de sécurité. Ces actions doivent inclure des campagnes d'information sur les menaces émergentes et les nouvelles techniques d'attaque, ainsi que des exercices pratiques tels que des simulations d'hameçonnage (phishing) ou d'ingénierie sociale.

2.3 GESTION DES BIENS

EX-SEC-GB-01 : Les données de l'ACOSS, y compris les données à caractère personnel, doivent être formellement identifiées, classifiées selon leur niveau de sensibilité. Elles doivent être isolées de manière logique et/ou physique des données d'autres clients ou tiers traitées par le Titulaire. Seul le personnel du Titulaire dûment habilité et autorisé à intervenir sur les projets ou services de l'ACOSS peut accéder à ces données, dans le strict respect du principe du besoin d'en connaître.

EX-SEC-GB-02 : Le Titulaire doit mettre en place des mesures techniques et organisationnelles pour tracer les accès aux données de l'ACOSS et détecter tout accès suspect.

EX-SEC-GB-03 : Le Titulaire doit mettre en oeuvre des procédures et dispositifs de sécurité pour se protéger contre le traitement non autorisé ou illégal, tout transfert non autorisé à un tiers, toute perte, destruction, altération ou divulgation accidentelle d'informations appartenant à l'ACOSS.

EX-SEC-GB-04 : Au terme de l'exécution du marché ou en cas de résiliation, le Titulaire restitue sans délai à l'acheteur une copie de l'intégralité des données confiées par lui dans le cadre de la prestation. Une fois la restitution effectuée, le Titulaire détruit de manière sécurisée et irréversible, dans un délai d'un mois, les éventuelles copies de données détenues dans son système d'information, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage. La restitution et la destruction des données

sont constatées par un procès-verbal daté et signé par le Titulaire. Les procédés de destruction sont conformes aux réglementations et aux normes en vigueur (par exemple NIST SP 800-88) et garantissent l'impossibilité de récupérer les données.

2.4 OBLIGATION DE CONFIDENTIALITÉ

EX-SEC-CONF-01 : Par dérogation à l'article 5.1.2 du CCAG-TIC, une information confidentielle désigne toute information de quelque nature (y inclus la méthodologie, la documentation, les informations ou le savoir-faire), sous quelque forme que ce soit (y inclus sous forme orale, écrite, magnétique ou électronique), sur tout support dont l'acheteur est propriétaire ou Titulaire, et qui est communiquée au Titulaire, ou obtenue de toute autre façon par ce dernier dans le cadre de ses relations avec l'acheteur. Le Titulaire et son personnel, et le cas échéant ses sous-traitants, ne peut l'utiliser que pour l'accomplissement des prestations prévues au marché.

Toutefois, n'est pas considérée confidentielle toute information :

- Qui était dans le domaine public au moment de sa divulgation ou que l'acheteur aurait lui-même rendue publique pendant l'exécution du marché ;
- Signalée comme présentant un caractère non confidentiel et relative aux prestations du marché ;
- Qui a été communiquée au Titulaire du marché par un tiers ayant légalement le droit de diffuser cette information, comme le prouvent des documents existant antérieurement à sa divulgation par l'acheteur.

2.5 TRAITEMENT DES INCIDENTS

EX-SEC-INC-01 : Les équipes de sécurité de l'ACOSS doivent être informées dans un délai maximum de 12h de tout incident de sécurité pouvant compromettre la sécurité et la confidentialité des données en rapport à tout projet de l'ACOSS. Cette alerte doit être réalisée par mail via à l'adresse de contact cos@acoss.fr. En cas d'urgence ou de de risque imminent pour la sécurité du SI de l'Acoss, l'alerte doit être immédiatement faite par téléphone au numéro 0986000951 puis doublée d'un mail à l'adresse cos@ACOSS.fr. De plus, la Déléguée à la Protection des Données de l'ACOSS doit être alertée si des données à caractère personnel du créancier sont compromises dans les conditions indiquées à l'annexe RGDPD fournie dans le cadre du marché via l'adresse de contact informatiqueetlibertes.acoss@acoss.fr.

EX-SEC-INC-02 : Le Titulaire doit documenter les procédures de réponse aux incidents et conserver une trace de tous les incidents traités en lien avec le présent marché, y compris les mesures correctives appliquées.

EX-SEC-INC-03 : Le Titulaire doit disposer d'un plan de gestion de crise informatique, intégrant la gestion des incidents de sécurité majeurs susceptibles d'affecter les données, les systèmes ou les services de l'ACOSS. Ce plan doit définir les rôles et responsabilités, les procédures d'escalade et de communication, les moyens de communication de crise, les scénarios de crise envisagés et les procédures associées pour la continuité et la reprise d'activité. Le plan de gestion de crise doit être testé au moins une fois par an.

2.6 CONTINUITÉ D'ACTIVITÉ

EX-SEC-CA-01 : Le Titulaire doit disposer d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA) documentés, à jour et adaptés aux services fournis à l'ACOSS. Le PCA doit décrire les dispositions prises pour assurer le maintien des activités essentielles réalisées pour le compte de l'ACOSS en cas de sinistre majeur. Le PRA doit décrire les procédures et les moyens techniques mis en œuvre pour la reconstruction des systèmes et la reprise des services après un sinistre, dans le respect des objectifs de temps de reprise (RTO) et de perte de données maximale admissible (RPO) définis dans le présent marché.

Le PCA et le PRA doivent être testés au moins une fois par an, à travers des exercices de simulation de sinistre, et mis à jour en fonction des résultats des tests, de l'évolution des services et de l'environnement technique.

SO-SEC-CA-01 : Il est souhaité que le Titulaire fournisse à l'ACOSS, sur demande, les rapports de tests du PCA et du PRA, ainsi qu'un résumé des plans d'actions d'amélioration issus de ces tests.

2.7 LIEU D'EXÉCUTION

EX-SEC-LOC-01 : Le Titulaire doit faire connaître à l'acheteur, sur sa demande, le lieu d'exécution des prestations. L'acheteur peut en suivre sur place le déroulement. L'accès aux lieux d'exécution est réservé aux seuls représentants de l'acheteur. Les personnes qu'il désigne à cet effet ont libre accès aux seules zones concernées par l'exécution des prestations prévues par le marché, dans le respect des consignes de sécurité prévues pour le site. Elles sont tenues aux obligations de confidentialité prévues au chapitre « Obligation de confidentialité ».

EX-SEC-LOC-02 : Lorsque le Titulaire envisage la réalisation d'une prestation objet du présent accord-cadre depuis un autre pays que la France, il en informe sans délai l'ACOSS. En effet, compte tenu des risques importants de sécurité qu'une telle situation est susceptible de favoriser, l'ACOSS doit pouvoir s'assurer au préalable que le Titulaire est en mesure de garantir une protection optimale du système d'information de l'ACOSS, des données et traitements qui lui sont confiés.

A cet effet, le Titulaire communique à l'ACOSS tous les éléments de nature à l'éclairer sur les conditions de mise en œuvre de cette prestation depuis l'étranger, prenant la forme d'un document spécifique répondant aux exigences particulières demandées par

l'ACOSS pour apporter toutes les garanties associées à ce type de prestation. De plus, si la prestation implique le traitement de données à caractère personnel, le Titulaire réalise une analyse d'impact relative à la protection des données (AIPD) et la fournit à l'acheteur.

En fonction des réponses fournies dans le document spécifique à la prestation réalisée dans un pays étranger, et au regard de la sensibilité de la prestation confiée, l'ACOSS apprécie si le niveau de garantie mis en œuvre est suffisant.

En cas d'acceptation, le document spécifique devient une pièce contractuelle, annexée au CCAP et les deux parties concluent les clauses contractuelles types de la commission européenne en matière de transfert de données personnelles hors de l'UE.

Il est interdit au Titulaire de réaliser une prestation relevant de l'exécution du présent accord-cadre depuis un pays autre que la France, dès lors que le Titulaire ne s'est pas vu notifié par l'ACOSS une décision expresse favorable et que le document spécifique n'a pas été signé par les deux parties.

L'ACOSS se réserve par ailleurs le droit de résilier le présent accord-cadre en cas de manquement du Titulaire à l'une des obligations définies ci-dessus, ce manquement constituant une faute particulièrement grave.

2.8 UTILISATION DE RESSOURCES BASÉES SUR L'INTELLIGENCE ARTIFICIELLE

EX-SEC-IA-01 – UTILISATION DE SYSTEMES D'INTELLIGENCE ARTIFICIELLE

1. Définition

Au sens du présent accord-cadre, un **système d'intelligence artificielle (SIA)** est entendu comme un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement et qui, pour des objectifs explicites ou implicites, déduit à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.

2. Interdiction des systèmes d'IA à risque inacceptable

La fourniture, le déploiement ou l'utilisation d'un SIA classé comme présentant un risque inacceptable au sens de l'article 5 du règlement (UE) 2024/1689 par le ou les titulaires, ses sous-traitants ou tout intervenant agissant pour son compte **est interdit**.

En cas d'identification d'une demande, d'un projet ou d'une pratique susceptible de s'apparenter à de la fourniture, à du déploiement ou à de l'utilisation d'un SIA à risque inacceptable, le ou les titulaire doit :

- suspendre immédiatement toute action liée à cette demande ou pratique ;
- alerter sans délai l'ACOSS en fournissant une description précise des éléments concernés ;
- coopérer pleinement à toute enquête interne ou externe visant à évaluer la conformité de la demande ou de la pratique avec le règlement (UE) 2024/1689.

3. Autorisation obligatoire préalable pour les autres systèmes

La fourniture, le déploiement ou l'utilisation d'un SIA par le ou les titulaires, ses sous-traitants ou tout intervenant agissant pour son compte **est strictement encadré et doit faire l'objet d'une autorisation préalable par l'ACOSS**.

Cette autorisation prend la forme **d'un accord écrit et préalable** de l'ACOSS sur demande motivée du titulaire.

Cette demande du titulaire devra préciser :

- Le type/nature de SIA utilisé au sens du règlement (UE) 2024/1689 ;
- Le modèle d'IA utilisé ;
- La finalité exacte de l'utilisation du SIA ;
- L'éditeur/fournisseur du SIA ;
- La nature des données susceptibles d'être traitées ;
- Les garanties techniques et organisationnelles mises en œuvre ;
- Les conditions d'hébergement, de sécurité et de confidentialité ;

- une évaluation des risques de sécurité et de conformité ;
- une AIPD le cas échéant ;
- La méthodologie d'entraînement, de réutilisation ou de diffusion des données traitées.

Au vu des informations transmises, **l'ACOSS en lien avec les services internes compétents** vérifie :

- que le titulaire respecte bien le périmètre d'usage limité et défini au présent accord-cadre ;
- que le SIA soumis à l'autorisation :
 - respecte les exigences prévues à la clause relative à la sécurité Informatique (article **XX** du présent accord cadre) ;
 - respecte les obligations issues du règlement (UE) 2024/1689 concernant l'intelligence artificielle et du règlement (UE) 2016/679 (RGPD) et la loi Informatique et Libertés ;
 - est hébergé dans des conditions garantissant un haut niveau de sécurité et offrant des garanties élevées en matière de confidentialité, d'intégrité et de traçabilité des données, avec la mise en œuvre des mesures d'anonymisation ou de pseudonymisation appropriées le cas échéant ;
 - est conforme aux principes d'éco-conception et de sobriété numérique.

A l'issue de l'examen, l'ACOSS notifie au titulaire une décision écrite qui peut être :

- une décision d'acceptation, éventuellement assortie de conditions et de restrictions d'usage valable que pour le périmètre décrit dans la demande. Toute autre utilisation devra refaire l'objet d'une demande ultérieure ;
- une décision de rejet.

L'absence de décision de l'ACOSS expresse vaut décision de refus d'autorisation.

L'ACOSS se réserve le droit à tout moment de refuser et donc d'interrompre l'utilisation de tout SIA en cours d'exécution du présent accord cadre, dont elle estime qu'il présente un risque notamment pour la sécurité et la confidentialité des données de l'ACOSS.

A défaut d'autorisation par l'ACOSS du SIA utilisé par un titulaire, cette utilisation est réputée non conforme au présent accord cadre et constitue un manquement du titulaire.

4. Protection des données, informations et documents

Le ou les titulaires s'engage à ce qu'aucune donnée, informations ou documents de nature confidentielle fournis par l'ACOSS ne soit divulgué, stocké ou traité par un SIA non maîtrisé. Un SIA est considéré comme non maîtrisé dans les cas suivants :

- L'hébergement ou la gestion des données ne garantit pas, de manière certaine et vérifiable, l'absence d'accès par des tiers non autorisés aux informations confidentielles ;
- L'ACOSS ne peut pas en auditer les conditions d'utilisation, à sa demande et sans restriction.

Il faut entendre par données, informations et documents confidentiels :

- a. Les données à caractère personnel :

Une donnée à caractère personnel désigne toute information se rapportant à une personne physique identifiée ou identifiable. Une personne physique peut être identifiée de manière directe (par exemple, par son nom et prénom) ou indirecte (par exemple, par un numéro, un identifiant en ligne, ou une donnée biométrique). Les données personnelles sont protégées par le RGPD et la loi Informatique et Libertés.

- b. Les autres données protégées par la loi, notamment :

- 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) ;
 - Ex : données qui se rapportent à la situation économique d'une entreprise en particulier, à sa santé financière ou à son crédit, en particulier l'ensemble des données relatives au chiffre d'affaires ou au niveau d'activité (ex : effectif salarié).

- Une donnée dont la divulgation porte atteinte à la sécurité publique, à la sécurité des personnes ou la sécurité du système d'information ;
 - Ex : données contenant des combinaisons de login/mot de passe permettant d'accéder à des applications, documents identifiant des failles de sécurité de notre SI, procédures d'évacuation d'un site etc.
- 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 ;
 - Ex : données ou combinaison d'informations faisant apparaître les méthodes ou la stratégie utilisées pour mettre à jour et combattre les tentatives de fraude, mettre en place des plans de contrôle, préciser nos opérations de cybersécurité etc.
- 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) ;
 - Ex : données relatives à la politique de placement et d'investissement de nature à rendre possible une spéculation financière qui pourrait avoir une incidence sur la gestion de la dette publique et la qualité du crédit public de la France (cf. conseil CADA no 20051762 du 26 mai 2005 relatifs au fonds de réserve des retraites).

5. Précisions relatives aux droits de propriété intellectuelle

A ce titre, en cas de recours à l'IA pour exécuter les prestations, les droits de propriété intellectuelle sont cédés et/ou concédés à l'ACOSS dans les mêmes conditions que les autres éléments produits par le Titulaire dans le cadre du marché, et tels que définis dans le présent CCAP et le CCAG-FCS qu'il s'agisse :

- Du contenu injecté (jeux de données, prompts etc.) ;
- Du contenu généré (textes, images, codes etc.) ;
- De tout autre élément inhérent à l'utilisation du SIA et/ou du modèle qui le compose.

Ainsi, le titulaire demeure, en toutes circonstances, responsable de la conformité des livrables qu'il produit, que cette production intègre un SIA, un modèle d'IA ou ait requis l'usage de l'IA, et garantit la titularité des droits transmis conformément aux besoins de l'ACOSS, lesquels comprennent en tout état de cause la possibilité de permettre la réutilisation sans surcoût des résultats ou des connaissances antérieures dans le cadre, notamment, d'une réversibilité.

Le titulaire s'engage notamment à conserver l'intégralité des contenus et élément inhérent à l'utilisation du SIA et/ou du modèle qui le compose, dans un format structuré, documenté et exploitable et cela sans dépendance technique.

A toutes fins utiles, il est rappelé que les modèles d'IA à usage général doivent permettre le respect du droit d'auteur (article 53 paragraphe 1 c du règlement (UE) 2024/1689).

6. Traçabilité, audit et information

L'ACOSS peut à tout moment auditer l'usage des SIA par le titulaire et demander la fourniture de preuves de conformité aux obligations en la matière.

L'ACOSS s'engage à informer le titulaire par écrit de la réalisation de l'audit avec un préavis minimal de 15 jours calendaires.

En cas de suspicion de manquement grave, d'incidence de sécurité ou d'atteinte à la confidentialité, l'audit peut être déclenché sans préavis.

L'ACOSS pourra confier cet audit en tout ou partie, à un tiers indépendant. Le titulaire ne peut s'opposer au recours à ce tiers auditeur, sauf en cas de conflit d'intérêts manifeste.

Le titulaire s'engage à coopérer pleinement avec l'ACOSS et à fournir tout document ou justificatif demandé par l'ACOSS lors de cet audit. Il désigne à ce titre un interlocuteur référent chargé de faciliter le déroulement de l'audit et de coordonner la transmission des informations demandées.

En dehors de tout audit, l'ACOSS peut être amenée à contrôler le titulaire à tout moment en cours d'exécution du marché. Ce dernier s'engage à fournir tout document ou justificatif demandé par l'ACOSS pour s'assurer de la conformité aux conditions du présent accord cadre.

Le titulaire doit informer immédiatement l'ACOSS de tout incident affectant la sécurité ou la confidentialité des données, y compris en cas d'utilisation non autorisée ou de fuite de données via un SIA.

Le titulaire s'engage à mettre en œuvre toutes les mesures correctives nécessaires pour limiter l'impact de l'incident.

7. Responsabilité

L'autorisation éventuelle accordée par l'ACOSS pour l'utilisation d'un SIA n'exonère en aucun cas le titulaire du respect intégral des dispositions du Règlement (UE) 2024/1689 relatif à l'intelligence artificielle, ni des autres obligations légales, réglementaires ou contractuelles applicables, notamment en matière de protection des données, de sécurité et de confidentialité.

En l'occurrence, l'autorisation d'utiliser un SIA accordée par l'ACOSS pourra s'accompagner d'un encadrement contractuel spécifique *sine qua non* lequel aura pour but de définir les obligations techniques et organisationnelles spécifiques visant à garantir la conformité légale et éthique du SIA, notamment si le SIA est à haut risque au sens du règlement précité.

Le titulaire demeure en tout état de cause pleinement responsable :

- des résultats produits avec l'assistance d'un SIA ;
- de tout manquement aux obligations de sécurité, de confidentialité ou de protection des données résultant de son utilisation.

L'utilisation d'un SIA ne saurait exonérer le titulaire de ses obligations contractuelles ni transférer de responsabilité à l'ACOSS.

8. Manquement du titulaire

En cas de non-respect par le titulaire des obligations visées au présent article, et indépendamment des sanctions pénales et administratives encourues, l'ACOSS pourra décider de résilier l'accord-cadre aux torts exclusifs du ou des titulaire(s), sans mise en demeure préalable et sans ouvrir droit à indemnités à quelque titre que ce soit.

Le titulaire supporte l'ensemble des conséquences financières, techniques et juridiques résultant de la résiliation fondée sur le présent article, sans préjudice du droit de l'ACOSS à réparation intégrale de son préjudice.

2.9 AUDIT DE SÉCURITÉ

EX-SEC-AUDIT-01 : L'ACOSS doit pouvoir, à tout moment, contrôler que les exigences de sécurité décrites au sein de la réponse du Titulaire, sont satisfaites par le Titulaire pour exécuter les prestations objet du présent accord-cadre.

Les audits pourront être réalisés par l'ACOSS à tout moment, ou délégués à un tiers expert présentant les compétences requises pour réaliser les opérations de vérification.

Le cas échéant, le contrôle s'effectuera selon les modalités décrites au sein de la réponse du Titulaire.

Nonobstant les alinéas précédents, dans le cas où l'ACOSS souhaite procéder à des contrôles au sein des locaux du Titulaire, l'ACOSS ou son délégataire procédera à cet audit après information du Titulaire, avec le respect d'un délai de préavis minimum de quinze (15) jours. En cas d'urgence, du fait par exemple de la survenance d'un incident grave de sécurité, l'ACOSS pourra réaliser l'audit de sécurité sur site sans délai de préavis.

En cas de pratique de tests intrusifs, une charte commune sera signée entre le Titulaire, l'exécutant de l'audit et l'ACOSS et sera annexée aux documents contractuels.

Si des vulnérabilités sont identifiées à l'issue de la conduite de l'audit, le Titulaire s'engage, sans surcoût, à mettre en œuvre un plan d'actions visant à éliminer ces vulnérabilités. Il s'engage à traiter en priorité les vulnérabilités engendrant les risques les plus élevés et à tenir informée quotidiennement l'ACOSS de l'avancée des travaux. Le Titulaire s'engage par ailleurs à prendre en charge les frais d'audit si celui-ci révèle des manquements avérés à ses obligations en matière de sécurité.