



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Agence de Services
et de Paiement

Direction des Soutiens Directs
Agriculteurs

POUVOIR ADJUDICATEUR :

Agence de services et de paiement (ASP)
2, rue du Maupas
87040 LIMOGES cedex 1

Annexe n°6 « Cadre de sécurité »



RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité



Agence de Services
et de Paiement

Table des matières

1	Conformité aux normes.....	4
1.1	Certification ISO 27001 de l'ASP.....	4
1.2	Homologation RGS	4
1.3	Autres conformités à respecter.....	4
2	Processus et organisation.....	5
3	Sécurité des infrastructures.....	5
3.1	CMDB.....	5
3.2	Authentification.....	5
3.3	Revue des comptes.....	5
4	Sécurité des développements.....	5
5	Mises à jour et correctifs de sécurité	6
6	Continuité de services	6
6.1	Disponibilité.....	6
6.2	Traçabilité	6
7	Protection des données et des échanges	6
7.1	Chiffrement des flux	6
7.2	Validation des données	6
7.3	Gestion du mécanisme de session	7
8	Réversibilité.....	7
9	Clauses de sécurité.....	8
9.1	Confidentialité	8
9.2	Audit de sécurité	8
9.3	Application des plans gouvernementaux.....	10
9.4	Politique de sécurité SI (PSSI) ASP.....	10
9.5	Charte de l'utilisateur du SI de l'ASP	10
9.6	Sécurité des développements et de la maintenance des applicatifs	11
9.7	Plan d'assurance sécurité	13



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

ASP

Agence de Services
et de Paiement

9.8	Localisation des données	13
9.9	Suivi des exigences de sécurité de la prestation.....	13
9.10	Gestion des changements et évolutions	14
9.11	Interventions dans les locaux de l'ASP	14
9.12	Conservation des données	14
9.13	Gestion des incidents de sécurité	15



1 Conformité aux normes

1.1 Certification ISO 27001 de l'ASP

Conformément aux obligations portant sur les Organismes Payeurs issues des règlements européens, il est attendu des tiers intervenants pour le compte de l'ASP qu'ils respectent les objectifs de sécurité définis par l'ASP pour les périmètres relevant de leurs responsabilités.

L'ASP a obtenu la certification ISO 27001 le 14 décembre 2016 pour trois années, sur le périmètre de la gestion des aides agricoles communautaire. Comme le prévoit la certification, l'ASP est audité annuellement pour le maintien de la certification, maintien qu'elle a obtenu en décembre 2022.

Dans le cadre du présent marché, le Titulaire s'engage au respect de la norme ISO 27001 en vigueur et de sa mise en œuvre, notamment dans le développement du nouveau SIGC. Le Titulaire doit fournir les éléments et preuves demandés par l'ASP ou lors des audits annuels de maintien de ladite certification.

1.2 Homologation RGS

Certains composants du Lac de données agricoles sont homologués RGS depuis novembre 2023 : la PFE et le Portail du LDA. L'échéance de révision de l'homologation RGS est au 31/12/2024.

Le Titulaire doit s'assurer du respect de la norme RGS en vigueur et de sa mise en œuvre. Le Titulaire doit fournir les éléments et preuves demandés par l'ASP ou lors d'audits pour l'homologation RGS.

Texte(s) de référence :

- L'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- L'arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.
- L'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques
- L'arrêté du 10 juin 2015 prorogeant les délais de mise en œuvre du référentiel général de sécurité.

1.3 Autres conformités à respecter

Le Titulaire doit s'assurer du respect de la directive NIS2 et de sa mise en œuvre en fournissant les éléments et preuves demandés par l'ASP ou lors d'audits de sécurité.

Le Titulaire doit se conformer aux exigences de traitement des alertes et des avis CERT France imposés par l'ASP. Un suivi de toutes les alertes doit être réalisé et une communication faite à l'ASP sur leur prise en compte.

2 Processus et organisation

Le Titulaire doit définir clairement chaque processus de sécurité (gestion des vulnérabilités matérielles, logicielles, des incidents, gestion de crise) et le formaliser dans le plan d'assurance sécurité (PAS) en précisant les interactions avec l'ASP et avec les titulaires des autres lots. De même les « exigences » de la PSSI de l'ASP doivent être formalisées dans le PAS.

3 Sécurité des infrastructures

3.1 CMDB

Le Titulaire doit mettre en place une CMDB sur la partie infrastructure mais aussi logicielle qui répertorie l'ensemble des actifs tels que définis par la PSSI ASP, avec la possibilité pour l'ASP d'y accéder. Un processus de mise à jour de cette CMDB doit être défini, formalisé et respecté pour bénéficier d'informations à jour.

3.2 Authentification

Le Titulaire doit gérer le mécanisme d'authentification. Le SI doit gérer les méthodes et les sessions REST. L'authentification doit être réalisée avec HTTPS.

Le SI doit permettre la mise en place d'un mode d'identification unique (SSO) pour les agents, et de l'authentification multi-facteurs (MFA), notamment afin de préparer la conformité avec NIS2.

Le Titulaire doit lutter contre les forces brutes, en mettant en place notamment des mécanismes CAPTCHA et/ou HONEYPOT.

Le Titulaire doit mettre en place une politique de gestion de mot de passe renforcée. Il ne doit pas utiliser des identifiants/mots de passe codés en dur.

Le Titulaire doit utiliser un algorithme de hashage renforcé.

3.3 Revue des comptes

Le Titulaire doit effectuer une revue au minimum deux fois par an des comptes à privilèges.

Il doit également procéder, au moins une fois par an, à un réexamen complet des droits d'accès (revue de comptes) et supprimer les comptes ou les autorisations d'accès qui ne sont plus nécessaires. Cette revue des accès concerne aussi bien les accès physiques que logiques. Une synthèse de cette revue doit être systématiquement fournie à l'ASP.

Cette revue doit aboutir à la production d'un document de synthèse auditable.

4 Sécurité des développements

Le Titulaire est seul responsable du maintien en condition de sécurité du système pendant toute la durée de l'accord-cadre. A cette fin, le Titulaire doit mettre en place une politique de sauvegarde du système d'information. Pour cela, les éléments à sauvegarder, la périodicité des sauvegardes, le lieu de sauvegarde et les droits d'accès qui y sont associés ainsi que les procédures de restaurations doivent avoir été clairement identifiés et documentés dans le Plan d'Assurance Sécurité (PAS) du Titulaire.

Le Titulaire doit toujours utiliser une gestion des erreurs. Les erreurs doivent être gérées côté serveur. Chaque message d'erreur doit être personnalisé et doit être loggé.

Les informations importantes doivent être loggées. Par contre, aucune information sensible ne peut être journalisée. En manière générale, le Titulaire doit produire des logs exploitables.



5 Mises à jour et correctifs de sécurité

Le Titulaire doit s'assurer que les versions de la couche logicielle sont maintenues et se coordonner avec l'ASP et le titulaire du Lot 4 pour l'application des montées de versions. Les correctifs de sécurité seront à appliquer selon les processus de gestion des vulnérabilités décrit dans le PAS.

Le Titulaire devra fournir à l'ASP une visibilité sur le suivi des incidents de sécurité sur la production, notamment dans la comitologie dédiée et décrite dans le PAS.

6 Continuité de services

6.1 Disponibilité

Le Titulaire garantit la continuité de fonctionnement de son environnement dédié aux développements et à la qualification.

6.2 Traçabilité

Tout système informatique doit créer, protéger et archiver une journalisation des événements système et applicatifs permettant par analyse fine de :

- Vérifier les connexions (réussite ou échec) au système ou à l'application et détecter les tentatives d'intrusions non autorisées ;
- Vérifier l'état du système (CPU, mémoire, etc.), disques (taux de remplissage, etc.), de l'application (nombre de licences atteint) ou détecter toute anomalie ou activité non autorisée concernant le système ou une application :
 - o Changement de droits sur un fichier ;
 - o Modification des privilèges d'un utilisateur ou groupe ;
 - o Ouverture d'un fichier sensible, activation d'une fonction spécifique.

Le Titulaire doit tracer l'ensemble de ces événements qui devront être horodatés, décrits comme échec ou succès et associés à l'utilisateur / processus qui les a commis.

Un point d'attention doit être mis sur les données "hautement personnelles" (NIR et RIB) et les actions effectuées par les comptes à privilèges.

Toute modification ou lecture des fonctions et informations d'audit doit être aussi tracée.

Enfin, par application du principe de moindre privilège, chaque journal doit être protégé et accessible uniquement à partir de comptes pour lesquels il existe des justifications opérationnelles (validées par l'ASP) à l'octroi de ces privilèges.

7 Protection des données et des échanges

7.1 Chiffrement des flux

Le Titulaire doit chiffrer tous les flux contenant des informations sensibles par des procédés fiables (SSH, TLS, Ipsec).

Les données suivantes doivent obligatoirement être chiffrées :

- Les flux d'authentification et d'administration,
- Le stockage des authentifiants utilisés

Le Titulaire doit signer et chiffrer les messages échangés par Web Services.

7.2 Validation des données

Le Titulaire doit mettre en place des mécanismes de contrôle et validation des données. Aucune donnée inconnue ne doit être acceptée sans validation. Les traitements effectués côté client doivent être rejoués côté serveur. Aucune requête dynamique ne doit être utilisée. Les paramètres utilisés par une redirection d'URL doivent être validés.



Le Titulaire doit encoder toutes les données utilisateurs et échapper toutes les données non sûres. Les sorties doivent être contrôlées. Le Titulaire doit valider toutes les données d'entrée fournies par l'utilisateur.

Le Titulaire doit valider le type MIME des téléchargements, la taille des téléchargements et les droits associés.

Le Titulaire doit utiliser un jeton pour valider les requêtes.

7.3 Gestion du mécanisme de session

Le Titulaire doit utiliser un ID de session durci. Après une connexion ou une déconnexion réussie, l'ID de session doit être recréé. Lors de la déconnexion ou après une période donnée, l'ID de session doit être détruit. Lors d'un changement d'identité, l'ID doit être redéfini.

Le Titulaire doit détecter les sessions frauduleuses. Il doit définir une fonctionnalité de déconnexion. Il doit pouvoir invalider une session utilisateur.

Le Titulaire doit communiquer un cookie de session. A la création d'un cookie, l'attribut « HTTPOnly » doit être défini. De même, l'attribut « secure » doit être défini pour chiffrer la transmission du cookie. Les cookies de session doivent avoir des domaines ou des chemins restrictifs.

8 Réversibilité

En cas de cessation de la relation contractuelle, quelle qu'en soit la cause, le titulaire s'engage à collaborer avec la MOA afin de faciliter la récupération/migration/arrêt du service :

- Apporter l'assistance nécessaire pour faciliter le transfert des données et des moyens de sécurité matériels et logiciels vers la MOA ou tout autre titulaire ;
- Accepter provisoirement l'accueil et le branchement de matériel du nouvel entrant afin de faciliter les opérations de transfert quel qu'en soit la nature (Données, ...)
- Garantir le service attendu et la sécurité des données et des applications pendant le transfert ;
- Assurer la prestation de service jusqu'au terme du marché/contrat.

En outre, la phase de réversibilité ne doit pas modifier la qualité, les termes et les conditions des services fournis durant le marché et définis dans la convention de service de chacun des lots.

En cas d'arrêt des prestations confiées à un ou plusieurs titulaires par la MOA, l'ensemble des matériels, logiciels et documentations confiés au(x) titulaire(s) doit être restitué.

Une restitution partielle peut être demandée par la MOA, en cas d'arrêt d'une partie des prestations avant la fin du marché. Dans ce cas, le titulaire en sera informé au moins un mois avant la fin des prestations.

À la fin de l'exécution du présent marché, le titulaire est tenu :

- De transférer à l'équipe du futur titulaire ou à la MOA, les informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet ;
- De préparer un support informatique défini par la MOA contenant tous les éléments (documentations, programmes, chaînes de compilation...) gérés par le titulaire actuel et qui seront, à l'issue de cette prestation, placés sous la responsabilité du futur titulaire ou de la MOA (cette mise à disposition devra être faite sous un format pouvant permettre au futur titulaire ou à la MOA d'installer, le cas échéant, l'ensemble de ces éléments sur une plateforme de son choix pour examen approfondi par celui-ci/celle-ci) ;
- D'assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels du futur titulaire ou de la MOA, avec travaux pratiques sur poste de travail, en présence de représentants de la MOA. Cette formation devra s'appuyer sur les documentations utilisateurs et techniques rédigées par le titulaire.

En particulier, au titre de cette prestation, le titulaire :

- Lance la prestation avec le futur titulaire et les représentants de la MOA ;
- Met à disposition tous les éléments et documents qu'il a produits ou lui ont été remis ;
- Présente l'ensemble des composants techniques ou fonctionnels du projet ;
- Répond aux questions du futur titulaire ou de la MOA concernant l'organisation pratique des configurations et des documents techniques sous 48 heures ;
- Présente l'organisation de la maintenance corrective actuelle et l'environnement de développement et d'exploitation (répertoires, installation, procédures mises en œuvre, périodicité et ordonnancement des opérations d'exploitation, etc.) ;



- Accueille, durant deux semaines, deux ou trois personnes du futur titulaire afin de leur permettre d'observer l'activité assurée par l'équipe projet en place (assistance téléphonique, exploitation de serveurs de développement, etc.) ;
- Communique au futur titulaire les réponses apportées aux demandes d'assistance téléphonique traitées.

9 Clauses de sécurité

Les clauses de sécurité détaillées ci-après sont applicables dès lors qu'elles sont opérationnellement réalisables. Le Titulaire apporte tous les motifs techniques, organisationnels et humains dans son mémoire technique permettant de justifier la non-application d'une ou plusieurs exigences définies ci-après.

9.1 Confidentialité

Principes généraux

Les informations gérées par l'Agence sont classifiées et marquées selon l'échelle ci-dessous.

Niveau	Nom
C4	Informations stratégiques et internes à l'Administration
C3	Informations concernant les bénéficiaires, agents ou intervenants et internes à l'Administration
C2	Informations ne contenant pas de données à caractère personnel et internes à l'Administration
C1	Informations publiques

Toute information non marquée est réputée classifiée C3.

Les informations classifiées C2 à C4 selon cette échelle ou dont le caractère « confidentiel » a été formellement spécifié sont réputées confidentielles. Ainsi, sont considérées comme confidentielles, les informations (notes, procédures et autres documents internes à l'Agence) et, le cas échéant, les données accessibles par le Titulaire ou mises à sa disposition dans le cadre de l'exécution de la prestation. Le Titulaire doit appliquer les mesures de sécurité permettant d'assurer la confidentialité des informations et données mises à sa disposition conformément à l'article confidentialité du CCAG TIC.

Les données intégrées ou générées sont utilisables dans le cadre de l'article « régime des données » du CCAG de référence. De même, la destruction des données s'opère en conformité à l'article « destruction des données » et « audit de sécurité » du CCAG TIC.

Engagement de confidentialité :

Le Titulaire s'engage à faire signer à chacun de ses intervenants, avant le démarrage de la prestation, l'engagement de confidentialité fourni par l'ASP. Sont considérés comme intervenants du Titulaire au titre du présent marché, ses personnels et ceux de ses éventuels sous-traitants directement impliqués dans l'exécution des prestations.

9.2 Audit de sécurité

Audits diligentés par l'Agence :



Le Titulaire s'engage, dans un délai de 15 jours ouvrés, à donner accès à tous les éléments en sa possession pour permettre un suivi par l'ASP des conditions de réalisation des prestations mentionnées dans le marché/contrat.

Par ailleurs, le Titulaire autorise l'ASP à réaliser ou faire réaliser par un tiers expert en la matière, des audits de sécurité (documentation, tests d'intrusion, audit de la sécurité de l'architecture des réseaux IT et des passerelles d'interconnexion, audit de la configuration des équipements de sécurité, audit de résilience PRA, test de conformité, etc.). En particulier, le Titulaire doit fournir les accès et informations permettant la réalisation de tests d'intrusions pour le déroulement des homologations RGS dont le pilotage est assuré par l'ASP. Enfin, l'ASP peut solliciter, sur demande, la participation des équipes du titulaire aux exercices de gestion de crise Cyber organisés par l'Agence.

Le Titulaire pourra refuser l'intervention d'un tiers après justification (ex. : conflit d'intérêt avéré). Le cas échéant, le Titulaire et l'ASP s'accorderont sur une solution alternative (ex. : audit par un tiers indépendant).

Lorsqu'un audit est diligenté par l'ASP, le plan d'audit (périmètre, fréquence, modalités de validation des résultats) sera fourni au Titulaire, dans un délai de 15 jours, avant le démarrage de l'audit.

Les constats d'audit doivent être pris en charge par le titulaire. À cet effet, le titulaire proposera à l'Agence un plan de prise en charge dans un délai de 15 jours ouvrés à compter de la réception du rapport d'audit définitif. Ce plan permettra d'établir le plan d'action visant à traiter les constats ainsi que leurs causes racines. Après approbation des deux parties, la mise en œuvre du plan d'action fera l'objet d'un suivi conjoint.

Le Titulaire doit intégrer dans le pilotage de son activité le suivi des actions SSI résultant d'un audit internes ou externes diligentés par l'ASP.

Audits diligentés par le Titulaire sur le périmètre de la prestation :

Lorsque le Titulaire diligente en interne des audits indépendants (ou s'il fait l'objet d'audit externes indépendants), régulièrement ou non, les résultats de ces audits peuvent être pris en compte par l'ASP sous certaines conditions. À cet effet, le Titulaire devra communiquer à l'Agence :

- le périmètre précis de l'audit, par rapport à la prestation réalisée pour le compte de l'ASP ;
- le référentiel d'audit utilisé ;
- les modalités de communication des résultats d'audit à l'Agence ;
- la fréquence de réalisation des audits (lorsqu'il s'agit d'audits récurrents) ;
- les éléments attestant de l'indépendance de l'audit (lorsqu'ils sont menés en interne).

L'Agence pourra prendre en compte ce type d'audit sous réserve qu'ils soient pertinents dans le contexte de la prestation. Le cas échéant, cette acceptation sera notifiée au Titulaire qui devra communiquer à l'Agence

- une copie du(des) rapport(s) d'audit ou les extraits concernant le périmètre de la prestation ;



- l'état de traitement des non-conformités concernant le périmètre de la prestation, sur demande de l'Agence.

9.3 Application des plans gouvernementaux

Le Titulaire s'engage à appliquer les mesures de sécurité issues des plans gouvernementaux (Vigipirate, Piranet) dès lors qu'elles concernent le périmètre des prestations. Dans un tel contexte, l'ASP communiquera régulièrement l'évolution des mesures au Titulaire, durant l'exécution du marché ; le cas échéant, un avenant au marché ou un ordre de service pourra être envisagé, selon l'impact sur les prestations.

Le Titulaire doit prendre en compte et assurer le suivi des alertes en cas d'événement de sécurité ou de réponse à une injonction de l'ANSSI (Agence Nationale de Sécurité des SI) après validation par l'ASP.

9.4 Politique de sécurité SI (PSSI) ASP

Principes généraux :

Le Titulaire s'engage à respecter les exigences applicables de la Politique de Sécurité SI (PSSI) de l'ASP qui concernent la prestation, mentionnées ci-après. Il doit s'inscrire dans les processus standards de gouvernance et de gestion de la sécurité tels que définis par l'ASP. Certaines règles pourront être adaptées au contexte spécifique de la prestation, après analyse des risques : les adaptations résultantes seront soumises à l'autorité concernée.

Le Titulaire notera plus particulièrement que :

- la connexion d'équipements tiers sur les réseaux informatiques de l'établissement est interdite, sauf autorisation formelle de la direction en charge de l'informatique ;
- la connexion d'un équipement présent sur le réseau de l'établissement à un autre réseau (privé ou à Internet via un modem ou un équipement similaire) est strictement interdite ;
- seuls les logiciels fournis et validés par la direction en charge de l'informatique de l'établissement peuvent être installés sur les postes de travail de l'ASP.

En cas d'évolution de la PSSI durant l'exécution du marché, modalités et délai de prise en compte des évolutions seront convenus entre l'ASP et le Titulaire. Pour les prestations concernées, cette prise en compte pourra impliquer une actualisation du Plan d'Assurance Sécurité (PAS).

9.5 Charte de l'utilisateur du SI de l'ASP

Dès lors qu'il utilise les moyens informatiques de l'Agence, le personnel intervenant pour le compte du Titulaire doit respecter la charte de l'utilisateur des SI de l'ASP. Cette charte sera fournie au Titulaire à la notification du marché par le service acheteur.

Le Titulaire veillera à ce que ses personnels concernés et, le cas échéant, celui de ses sous-traitants signent et respectent cette charte. En cas d'évolution de la charte sur la période d'exécution du marché, la nouvelle version sera communiquée au Titulaire, lequel devra veiller à ce qu'elle soit signée par ses personnels concernés.

9.6 Sécurité des développements et de la maintenance des applicatifs

Principes généraux :

Le Titulaire s'engage à mettre en œuvre les principes de « privacy by design » et de « privacy by default ».

Le Titulaire est responsable de la conformité légale et réglementaire des systèmes qu'il met en œuvre (en particulier en matière de licences logicielles). A contrario, l'ASP est responsable des systèmes et outils qu'elle met à disposition du Titulaire dans le cadre de l'exécution du marché.

Toutes les données utilisées et/ou produites dans le cadre des développements informatiques de l'ASP devront faire l'objet d'un effacement sécurisé avant l'affectation des matériels ayant supporté ces développements, à un autre usage.

Le Titulaire ne pourra avoir accès qu'aux ressources (sources, documents, outils ...) dont il a la stricte nécessité. Le Titulaire appliquera les règles de développement sécurisé de l'Agence précisées au sein de cette annexe. En cas d'évolution des règles, Titulaire et Agence s'accorderont sur un délai de mise en application cohérent au regard desdites évolutions. Si le Titulaire dispose de ses propres règles de développement sécurisé, celles-ci pourront être utilisées si, et seulement si, les règles d'équivalence ont été documentées et approuvées par l'Agence.

Innocuité des systèmes et des livrables :

Le Titulaire mettra en œuvre les mesures permettant de garantir l'innocuité des systèmes utilisés dans le cadre de la production applicative et des livrables à destination de l'ASP. Il veillera en particulier à ce que les livrables produits soient exempts de « codes malicieux », de « fonctionnalités cachées », de « portes dérobées », et qu'ils ne permettent aucune fuite d'information.

Contrôles :

La sécurité des développements fera l'objet de contrôles par l'ASP :

Les codes sources devront être exempts de vulnérabilités et de code malveillant.

Les contrôles réalisés en interne par le Titulaire devront être basés sur des règles au moins équivalentes à celles utilisées par l'Agence. Une preuve de ces contrôles devra être tenue à disposition de l'ASP. Le résultat de ces contrôles sera présenté à l'Agence dans le cadre du suivi de la prestation.

Gestion des vulnérabilités :

Le Titulaire s'engage à traiter les vulnérabilités découvertes dans l'ensemble du SI qu'il exploite dans le cadre du présent marché. À cet effet, il procèdera à une évaluation des vulnérabilités selon l'échelle CVSS en vigueur. Une échelle alternative pourra être utilisée,



sous réserve d'un accord préalable de l'ASP. Dans l'attente du traitement définitif d'une vulnérabilité, des mesures palliatives (traitement temporaire, mesure de limitation de risque) devront être proposées à l'ASP.

Environnement de travail :

Le Titulaire doit veiller à appliquer les mises à jour de sécurité des matériels et logiciels qu'il met en œuvre dans le cadre de la prestation. Il ne peut déroger à cette règle que sur instruction formelle de l'ASP. Dans le cas où la prestation s'effectuerait dans les locaux du Titulaire en utilisant des ressources informatiques de l'établissement, le Titulaire devra mettre en œuvre les mesures de sécurité permettant de garantir que seuls ses collaborateurs désignés pour la prestation sont en mesure d'utiliser les moyens mis à disposition par l'ASP.

L'ASP envisage la mise en place d'un SOC mutualisé. Dans ce cadre, les modalités d'interconnexion des SI seront définies en cours d'exécution du marché.

Environnement de développement :

Le Titulaire s'engage à :

- dédier un environnement si possible physique, à défaut logique de développement aux prestations objet du présent marché ;
- informer formellement l'ASP de tout changement concernant l'environnement de développement susceptible d'impacter la sécurité.

Dispositions propres aux développements :

Le Titulaire doit assurer la sécurité des développements conformément à l'état de l'art et à la politique de sécurité de l'ASP dans chacune des technologies mises en œuvre. Il doit en particulier :

- maintenir l'environnement applicatif en tenant compte des recommandations de l'ASP ;
- assurer un contrôle rigoureux des entrées utilisateurs ;
- assurer un cloisonnement strict des accès des utilisateurs ;
- sécuriser les accès aux fonctions d'administration ;
- installer ou activer uniquement les fonctions nécessaires et appliquer le principe du moindre privilège ;
- respecter les recommandations de l'OWASP, pour les technologies web ;
- mener, dans le cadre des phases de recette, une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité, pour les codes pour lesquels cela s'applique ;
- corriger à sa charge les éventuelles anomalies détectées lors de la revue de code ;
- implémenter des mesures de protection face aux attaques, en particulier les attaques par injection ou par dépassement de capacité ;
- assurer la gestion des erreurs applicatives (la remontée et le traitement ne doivent en aucun cas présenter d'informations techniques à l'utilisateur) ;
- implémenter des journaux d'événements requis ;
- fournir à l'ASP l'ensemble des éléments utilisés dans le cadre des développements permettant à l'ASP de construire les applications ;



- prouver que les éléments externes utilisés n'introduisent pas de vulnérabilités au sein des applications ;
- identifier l'ensemble des flux avec des entités externes des applications. Ces flux devront être validés conjointement entre les équipes du titulaire et de l'ASP ;
- utiliser des mesures cryptographiques conformes aux directives nationales de l'ANSSI.

9.7 Plan d'assurance sécurité

Le Titulaire s'engage à exécuter ses obligations en matière de sécurité des systèmes d'information selon le Plan d'Assurance Sécurité (PAS).

Le Titulaire est responsable de la rédaction initiale du PAS ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité de l'ASP pendant toute la durée de la prestation. Il doit en particulier définir la mise en place des processus et de l'organisation permettant le déploiement d'une gouvernance opérationnelle de la SSI conformément aux exigences de sécurité de l'ASP.

Le projet de Plan d'Assurance Sécurité établi conformément à la trame fournie par l'ASP, qui s'applique aux équipes du Titulaire et aux sous-traitants éventuels.

Le PAS, à valeur contractuelle, sera finalisé dans un délai de 3 mois, à compter de la notification. Le PAS fera l'objet d'une révision annuelle par les deux Parties.

9.8 Localisation des données

Afin d'assurer des garanties de sauvegarde et de restauration, de confidentialité, de sécurité logique pour la gestion spécifique des identités et des accès, de sécurité physique du site d'hébergement, d'intégrité des données ou de propriété des données, le Titulaire s'assure de respecter les dispositions suivantes.

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité de l'ASP et à la législation relative à la protection des données à caractère personnel.

Dans le cadre du présent marché, l'ASP souhaite que les données soient hébergées et traitées sur le territoire national. Le Titulaire garantit que le transfert des données n'est possible qu'au sein des pays membres de l'Union européenne et s'engage à informer l'ASP au préalable (délai de un mois) si les lieux d'hébergement devaient être modifiés.

Le Titulaire s'engage à communiquer à l'ASP, la liste de tous les lieux de stockages de données (sites d'hébergements principaux, sites de secours, ...).

9.9 Suivi des exigences de sécurité de la prestation

Le Titulaire s'engage à documenter le processus de gestion des incidents de sécurité conformément à la procédure en vigueur au sein de l'ASP.

Le Titulaire s'engage à participer aux comités permettant d'assurer le suivi des exigences de sécurité applicables dans le cadre de la prestation.



Les ordres du jour de ces comités de suivi sont définis conjointement par le Titulaire et l'ASP et sont formalisés par le Titulaire. Les points sécurité à traiter dans ces réunions sont, a minima :

- le suivi de la couverture des exigences et clauses de sécurité ;
- le suivi des niveaux de services exigés par les engagements de service ;
- l'analyse des indicateurs portant sur :
 - les exigences et clauses de sécurité ;
 - les niveaux des engagements de service ;
 - les incidents impactant les services et prestations.
- le suivi des plans d'amélioration ;
- l'information de l'Agence quant aux changements apportés aux mesures de sécurité, le cas échéant.

Les comptes rendus sont formalisés par le Titulaire et communiqués à l'ASP, au plus tard 5 jours ouvrés après le comité.

9.10 Gestion des changements et évolutions

Le Titulaire devra informer l'ASP de tout changement ayant une incidence sur la sécurité de l'information, sur le périmètre de la prestation. Lorsque ce changement est de nature à introduire ou augmenter les risques en matière de sécurité de l'information, le changement sera subordonné à l'accord formel de l'ASP.

Le Titulaire devra tracer les demandes de changement conformément au référentiel ITIL ou à un des cadres de gestion des services IT équivalent,

9.11 Interventions dans les locaux de l'ASP

La Titulaire devra respecter les règles de sécurité spécifiques à l'accès aux locaux définis par l'ASP, notamment, l'accès limité aux zones d'intervention définies par le marché/contrat et le port apparent du badge, cela pendant toute la prestation.

9.12 Conservation des données

Le Titulaire s'engage sur l'intégrité et la confidentialité des données qui lui sont confiées pour l'exécution de sa prestation. Il appartient en particulier au Titulaire de faire des sauvegardes des informations de l'ASP et de gérer ces sauvegardes de manière à permettre une reprise en cas d'incident, en particulier pour le code source, les spécifications, etc....

Le Titulaire présentera notamment les mesures proposées pour sécuriser la phase de transfert du système (transfert de matériels ou de logiciels) ainsi que les procédures de contrôle de la sécurité du transfert mises en œuvre.

9.13 Gestion des incidents de sécurité

Documentation :

Le Titulaire doit disposer d'une documentation lui permettant d'assurer une gestion adaptée des incidents de sécurité. Celle-ci doit en particulier décrire les modalités :

- d'analyse et de qualification de l'incident ;
- d'identification, d'acquisition / de collecte et de préservation des preuves numériques ;
- de signalement de tout incident impactant l'ASP, au(x) point(s) de contact définis par l'ASP.

Pour les cas concernant – ou ayant un impact sur – l'ASP, les actions nécessaires à la résolution de l'incident devront être documentées par le Titulaire et tenues à disposition de l'ASP.

Points de contact, modalités de signalement et d'échange en cas d'incidents de sécurité :

Les incidents de sécurité devront être signalés aux points de contact de l'Agence qui seront communiqués formellement au Titulaire (courriel et téléphonique) au lancement de la prestation.

Le Titulaire communiquera à l'ASP la liste de ses points de contacts (courriel et téléphonique) en matière de gestion des incidents de sécurité. Il veillera à communiquer à l'Agence tout changement apporté à cette liste. En cas de crise, des modalités d'échange spécifiques pourront être mises en œuvre entre l'Agence et le Titulaire, si cela s'avère nécessaire (ex. : compromission de messagerie, indisponibilité des systèmes de téléphonie fixe, ...).

Délais de signalement à l'ASP :

Tout incident de sécurité survenant sur le périmètre de la prestation devra être notifié à l'ASP dans les 24h suivant sa détection. En cas de cyber-attaque impactant tout ou partie de ses systèmes d'information, le Titulaire devra alerter le(s) point(s) de contact de l'ASP mentionnés supra, dans les meilleurs délais possibles, considérant la situation. En tout état de cause, le délai de signalement à l'ASP ne pourra excéder 48h sous peine d'application de pénalités prévues à la convention de service.

Dispositions spécifiques aux cas de crise :

Le Titulaire s'engage à informer l'ASP de l'évolution de la situation dans les meilleurs délais. En cas d'attaque informatique, le Titulaire s'engage à communiquer à l'Agence, dès que possible :

- les éléments macroscopiques relatifs à l'attaque (en particulier vecteur et outillage utilisés) ;
- les éventuels vecteurs de risques pour l'Agence, s'ils sont identifiés (ex. : courriels ou fichiers suspects adressés à l'Agence et identifiés lors des phases d'analyse de l'attaque) ;
- les éventuels indicateurs de compromission, s'ils sont identifiés.

Mesures d'isolement des SI et gestion du retour à la normale :



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

ASP

**Agence de Services
et de Paiement**

En cas d'incident de sécurité présentant un risque non maîtrisé de propagation aux systèmes d'information de l'ASP, le Titulaire devra, sauf contre-indication formelle ASP, isoler ses SI de ceux de l'Agence.

En fonction de l'urgence de la situation et des niveaux de risque évalués par l'ASP, l'Agence se réserve le droit d'isoler ses propres SI de ceux du Titulaire et/ou de ses éventuels sous-traitants. Cette mesure pourra être mise en œuvre de façon unilatérale, immédiate et sans préavis. Lorsqu'une mesure d'isolement conduit à rompre un canal de communication utilisé dans la gestion de crise, des moyens d'échanges palliatifs doivent être déterminés d'un commun accord ASP - Titulaire.

La réouverture des communications pourra être progressive. Elle sera conditionnée à la transmission d'un engagement formel du Titulaire quant à la circonscription, à la maîtrise ou la fin de l'incident. Cet engagement devra permettre à l'Agence une prise de décision circonstanciée quant à l'arrêt des mesures d'isolement. Le candidat précisera dans son offre sa politique en matière de recours à un prestataire de réponse aux incidents de sécurité (PRIS) qualifié.

Mesures de capitalisation :

Sauf accord formel de l'ASP, lorsqu'un incident introduit un impact majeur ou critique pour l'Agence, le Titulaire organisera un retour d'expérience en y associant l'ASP dans les 3 mois suivant le retour à la normale.