

Annexe 5 –

Exigences SSI applicables au développement et à la maintenance applicative du système PING

1. Sécurité des développements applicatifs, de la maintenance

- 1.1 Le Titulaire est tenu de se conformer à l'état de l'art en matière de sécurité des technologies mises en œuvre pour effectuer des développements.
- 1.2 Pour la mise en œuvre de technologies web, les développements s'appuient sur les recommandations de l'OWASP (Open Web Application Security Project).
- 1.3 Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.
- 1.4 Le Titulaire autorise le Shom ou un organisme de l'Etat, via un tiers mandaté le cas échéant, à effectuer les revues de codes afférentes à ces exigences.
- 1.5 Les modifications des sources des logiciels doivent être suivies dans un outil de contrôle de versions permettant de tracer les modifications effectuées et d'identifier leur auteur.
- 1.6 Les applications sur Internet doivent disposer d'un pare-feu applicatif.
- 1.7 La démarche de test doit inclure une vérification de robustesse de l'application et la qualification de ses fonctions de sécurité.
- 1.8 La modification du SI en exploitation nécessite au préalable :
 - la validation de la modification sur la plateforme de pré-production représentative du système en exploitation ;
 - la vérification différentielle que les modifications effectuées sont rattachées à des évolutions prévues ;
 - l'application d'un plan de test de non régression sur les fonctions critiques du système ;
 - l'application systématique d'un plan de test de non régression sur les échanges avec les autres systèmes opérationnels ;
 - l'archivage des modifications apportées.

- 1.9 Les environnements de développement doivent être protégés contre les intrusions afin de garantir l'intégrité et, si nécessaire, la confidentialité des codes sources.
- 1.10 Le recours à des prestataires de service de sécurité (services de filtrage tels que protection contre le déni de service, lutte contre le spam, gestion de firewalls ; de détection d'incidents ; de tests de vulnérabilité ou de conformité, etc.) qualifiés par l'ANSSI est obligatoire et est autorisée que par des entreprises opérant depuis le territoire national.
- 1.11 Les prestations d'infogérance à distance sont réalisées sur et depuis le territoire national.
- 1.12 La liaison de télémaintenance est sécurisée de bout en bout jusqu'au système ou l'équipement cible.
- 1.13 Les accès aux interfaces de configuration et d'administration à distance ne doivent être accessibles qu'aux personnes autorisées.
- 1.14 Le Titulaire s'engage à fournir une liste, régulièrement mise à jour, des personnels intervenant sur le SI ainsi que leur niveau d'habilitation (types d'accès et ressources concernées du client).
- 1.15 Le Titulaire précise les qualifications et expériences, formations et sensibilisations dans le domaine de la SSI des personnels en charge des prestations.
- 1.16 Les obligations du Titulaire, y compris les clauses de sécurité, s'appliquent intégralement à ses sous-traitants et sous sa responsabilité. Le Titulaire doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché et doit s'assurer du respect de ces obligations par ses sous-traitants.

2. Produits sur étagère

- 2.1 Dans le cas d'un emploi de produits sur étagère non paramétrable, le Titulaire fournit au Shom un dossier de sécurité du produit sur étagère avec :
 - une cinématique claire du processus de sécurité du produit,
 - des propositions organisationnelles et techniques à mettre en place contre les menaces identifiées critiques ou majeures.

2.2 Le Titulaire doit configurer les produits utilisés de façon à contrer leurs failles de sécurité intrinsèques et selon le strict besoin fonctionnel du SI. Cette configuration doit au moins inclure :

- la fermeture des ports inutilisés ;
- la suppression des logiciels ou fonctions inutiles (sources, binaires, byte-codes, scripts, fichiers de paramétrage) ;
- la désactivation des services inutiles ;
- la configuration des services pour qu'ils n'accèdent qu'au strict besoin pour le SI ;
- la restriction des accès aux données gérées ou utilisées par le produit (fichier, répertoire, registre, ...) aux seuls profils utilisateurs en ayant le besoin.

- 2.3 Les composants logiciels commerciaux doivent disposer d'une licence valide assortie de la mise à disposition des correctifs de sécurité.

3. Authentification d'un utilisateur

- 3.1 Le SI doit être paramétrable sur les critères de longueur et de complexité des secrets (mot de passe de n caractères, chiffres, caractères spéciaux, certificats...).
- 3.2 Les mots de passe ne doivent pas être stockés en clair (par exemple dans un fichier ou base de données) ni transiter en clair sur les réseaux (sauf mots de passe à usage unique). Ils sont chiffrés en utilisant des mécanismes à l'état de l'art. Le SI doit stocker les informations d'authentification de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés (droits d'accès, limités au strict besoin, sur les fichiers utilisés pour l'authentification).
- 3.3 Le SI doit offrir des mécanismes techniques pour imposer et contrôler que les secrets choisis par les utilisateurs (mots de passe par exemple) respectent des critères de longueur et de complexité définis par un usager possédant les privilèges d'administrer la stratégie de sécurité des mots de passe. Les secrets ne respectant pas ces critères doivent être refusés par le SI.
- 3.4 L'authentification sur le SI doit s'appuyer sur des identifiants personnels afin de permettre une imputabilité individuelle des accès et des actions. Les comptes de personnels sont donc affectés individuellement. Les comptes de service ne peuvent être accédés qu'après une authentification personnelle.
- 3.5 Une authentification forte (2 facteurs si possible) est requise pour l'administration du SI et pour la gestion et la production d'informations sensibles.

4. Gestion des profils et comptes utilisateurs du SI

- 4.1 La gestion des droits d'accès applicatif et des autres informations nécessaires au bon fonctionnement de l'outil doit être faite par l'outil lui-même au travers une gestion centralisée des comptes utilisateurs et de leurs privilèges ce qui permet de disposer d'un référentiel unique et maintenu dans le temps.
- 4.2 Le SI doit offrir la capacité de créer des profils, auxquels sont associés des privilèges qui dissocient les prérogatives de chacune des catégories d'utilisateur, selon le principe du moindre privilège.
- 4.3 Lorsque la fonction d'un personnel nécessite des privilèges particuliers, un compte supplémentaire avec les stricts privilèges nécessaires est créé pour cet utilisateur. Les différents comptes à privilège d'un même personnel sont protégés par un mot de passe distinct du compte sans privilège. Les comptes à privilèges sont restreints à l'usage de ces privilèges.
- 4.4 Le SI doit offrir à un profil spécifique les moyens de désactiver et/ou supprimer les comptes inutilisés ou usurpés.

5. Authentification au système hébergé

- 5.1 Pour chaque interface d'accès au système (Interface Homme-Machine, interface entre applications), le Titulaire, en concertation avec l'Hébergeur, décrit :
 - les mécanismes d'authentification mis en œuvre (protocoles, algorithmes de hachage et de chiffrement utilisés) ;
 - la liste exhaustive des comptes d'accès existants ainsi que des rôles et privilèges qui y sont associés.
- 5.2 Les moyens d'authentification associés aux interfaces doivent être interopérables tant au niveau des applications clientes (par exemple navigateurs web) que des systèmes d'exploitation.
- 5.3 Les interfaces d'accès aux fonctionnalités bas niveau (exemple : configuration du BIOS) doivent impérativement authentifier un utilisateur (mise en place d'un mot de passe pour l'utilitaire de configuration du BIOS).
- 5.4 Les identifiants des comptes d'accès sont nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par le donneur d'ordres. Dans ce

cas, le Titulaire présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité.

5.5 L'utilisation de mots de passe constructeur ou par défaut est interdite.

5.6 L'utilisation de protocoles dont l'authentification est en clair est interdite.

6. Session de connexion au SI

6.1 La session de connexion doit se verrouiller après une durée d'inactivité paramétrable pour l'ensemble du SI par un administrateur technique.

7. Gestion des traces

7.1 Le SI doit être conçu pour enregistrer et restituer toutes les actions sur le système sans que l'utilisateur puisse modifier ces traces.

7.2 Le SI doit remonter une alarme à destination d'un profil de sécurité lors du blocage d'un poste dû à 5 successions d'échecs d'authentification.

8. Imputabilité, traçabilité

8.1 Les informations suivantes doivent être enregistrées :

- entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
- actions qui tentent d'exercer des droits d'accès à un objet soumis à l'Administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative ;
- création/suppression d'un objet soumis à l'Administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
- actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

9. Journaux d'événements et conservation des traces

- 9.1 Le Titulaire applique les recommandations de l'ANSSI : Note technique - Recommandations de sécurité pour la mise en œuvre d'un système de journalisation –Réf ANSSI-PA-012/ANSSI/SDE du 28/01/2022 .
- 9.2 Les dispositifs de journalisation doivent permettre de conserver une trace des événements de sécurité observés sur le système d'information durant 12 mois glissants.

10. Confidentialité et intégrité des flux

- 10.1 Tous les flux d'Administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec, etc.), garantissant la confidentialité et l'intégrité des données.
- 10.2 De façon générale, tous les flux contenant des informations et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties (https).
- 10.3 Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.
- 10.4 Le Titulaire indique l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'Administration.

11. Prévention, gestion des incidents et alertes

- 11.1 Le Titulaire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations dans son domaine d'intervention.
- 11.2 Le Titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer le Shom des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.
- 11.3 Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

- 11.4 Le Titulaire assure la veille SSI sur les composants applicatifs du SI et sur les vulnérabilités éventuelles.
- 11.5 Le Titulaire informe par mail le Shom de toutes les alertes SSI liées aux composants applicatifs ainsi que le niveau de risque encouru par le SI dans son environnement de production et les précautions immédiates à prendre pour corriger les vulnérabilités ou limiter les impacts potentiels.
- 11.6 Lorsque le correctif de la faille de sécurité est accompagné d'une mise à jour évolutive des composants impactés, le Titulaire réalise une analyse d'impact.
- 11.7 Le Titulaire vérifie et teste les patches de sécurité sur sa propre plateforme de développement, il informe le Shom des résultats de non régression des fonctionnalités du SI, livre le guide d'installation et les patches de sécurité.
- 11.8 Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré-production.
- 11.9 La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du Titulaire, de l'Hébergeur et le chef de projet responsable de l'application hébergée.
- 11.10 Le Titulaire doit mettre à jour le Plan d'Assurance Sécurité (PAS) avec la liste des correctifs de sécurité appliqués et communiquer au Shom la version actualisée du document.
- 11.11 En cas d'alerte donnée par les équipes d'experts du Titulaire ou de l'Hébergeur ou par le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux Attaques informatiques) ou par le CALID (Centre d'analyse de lutte informatique défensive du ministère des armées), le Shom doit être notifié par téléphone et courrier électronique avant toute opération. La décision de l'action n'est prise que par le Shom (le Shom désignera les personnes autorisées à décider).
- 11.12 Le Titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (heures ouvrées et non ouvrées) permettant au Shom de suivre le traitement d'une alerte.
- 11.13 Dans le cadre de l'application de plans gouvernementaux, le Premier Ministre peut décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes

visant les systèmes d'information de l'État ou les systèmes. Dans le cadre des prestations, le Titulaire pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par l'Administration. Ces mesures sont susceptibles d'évoluer. Les modifications seront régulièrement transmises durant l'exécution du marché.

11.14 Prévention d'une attaque : le Titulaire indique dans le plan d'assurance sécurité (PAS) :

- un contact technique (ou plusieurs) clairement identifié, joignable tous les jours ouvrés de l'année ;
- un contact décisionnel (ou plusieurs) clairement identifié, joignable tous les jours de l'année.

12. Réversibilité

Se référer au document principal du CCTP.

13. Sécurité de défense – exigences réglementaires

13.1 Le SI traitera des informations sensibles non classifiées de défense et sera homologué au niveau standard. En conséquence, le Shom veillera à la bonne exécution des prestations, au respect des règles SSI, notamment à la confidentialité à la disponibilité, et à l'intégrité des données, et demande au Titulaire de s'engager sur le respect de ces règles.

13.2 Certaines informations contenues dans le SI étant d'un niveau de protection « sensible », le Titulaire s'engage à appliquer la législation et la réglementation en la matière en se conformant notamment aux principaux textes référencés ci-dessous :

- Instruction générale interministérielle n° 1300/SGDN/PSE/SSD du 09 août 2021,
- relative à la protection du secret et des informations concernant la Défense Nationale et la Sûreté de l'État,
- Instruction Interministérielle 901 du 06 janvier 2022 portant sur la protection des systèmes d'information sensibles,
- Instruction ministérielle n° 900 DEF/CAB/DR du 15 mars 2021 relative à la protection du secret au sein du ministère de la défense (diffusion restreinte - consultable auprès du Shom).

14. Sécurité de défense - Données transmises au Titulaire

- 14.1 Si l'échange de données sensibles entre le Titulaire et le Shom s'avère nécessaire, celles-ci doivent être chiffrées via le logiciel de chiffrement fourni par le Shom. Dès la notification du marché, le Titulaire communique au Shom les informations requises en vue de la délivrance des clés cryptographiques individuelles nécessaires à l'utilisation de cet outil.
- 14.2 Le Titulaire n'utilise pas les données du SI à des fins autres que celles spécifiées au marché.
- 14.3 Il est interdit au Titulaire de communiquer toutes les données à des tiers n'intervenant pas au titre du marché, qu'il s'agisse de personnes physiques ou morales.
- 14.4 Le Titulaire prévient le Shom en cas d'atteinte à la sécurité des données transmises.
- 14.5 Sur demande écrite du Shom, le Titulaire cesse d'utiliser les données transmises par le Shom et procède à leur destruction ainsi qu'à celle des copies éventuellement réalisées.
- 14.6 En fin de marché, le Titulaire procède à la destruction de toutes les données (et des copies éventuelles).
- 14.7 Pour toute destruction des données du SI par le Titulaire le Shom demande que l'un des traitements suivants soit appliqué à tous les disques contenant des données du SI :
- soit destruction physique du support
 - soit utilisation de la fonction « Effacement sécurisé » du logiciel d'effacement fourni par le Shom.
- La réalisation du traitement est certifiée par un document formel émis par l'officier de sécurité des systèmes d'information (OSSI) du Titulaire.

15. Plan d'assurance de sécurité

- 15.1 Le Titulaire fournira un plan d'assurance de sécurité (PAS) qui décrit les dispositions prises par le Titulaire pour répondre aux exigences de sécurité pendant toute la durée de la prestation. La version initiale du PAS est celle annexée au mémoire technique du Titulaire. Le PAS sera mis à jour par le Titulaire à chaque évolution pendant toute la durée des prestations. Le PAS est un livrable qui sera soumis à la validation du Shom.
- 15.2 Le plan d'assurance sécurité sera rédigé conformément aux recommandations du guide de l'ANSSI « MAÎTRISER LES RISQUES DE L'INFOGÉRANCE - Externalisation des systèmes d'information »¹ telles présentées en appendice.
- 15.3 Le Titulaire s'engage à exécuter ses obligations selon le PAS validé par le Shom.

16. Procédures d'exploitation de la sécurité (PES)

- 16.1 Le Titulaire participera, pour les aspects dont il a la charge, à la mise au point des procédures d'exploitation de la sécurité (PES) ou des instructions techniques d'emploi (ITE). Ces documents décrivent en particulier les points suivants :
- l'organisation et l'administration de la sécurité du système ;
 - le niveau de protection des données traitées et les responsabilités encourues ;
 - la gestion des accès des personnels, tant physiques que logiques ;
 - la gestion, la circulation et la destruction des supports ;
 - la politique de sécurité du système déclinée pour les utilisateurs ;
 - le plan de mise en marche, d'arrêt du système, de configuration ;
 - les procédures de sauvegarde et de destruction d'urgence ;

¹ https://cyber.gouv.fr/sites/default/files/IMG/pdf/2010-12-03_Guide_externalisation.pdf

- les fiches réflexes en cas d'incidents de sécurité.

Les PES et ITE sont accessibles aux utilisateurs et aux acteurs concernés par la mise en œuvre du système (administrateurs,...). Les PES et ITE sont des livrables qui seront soumis à la validation du Shom.

Le niveau de protection des procédures d'exploitation et de la documentation décrivant les éléments concourant directement à la sécurité du SI (paramétrage des dispositifs de sécurité, ...) est déterminé par l'OSSI du Shom. Un modèle de PES publié par l'ANSSI est accessible sur son site à l'adresse :

<https://cyber.gouv.fr/publications/lhomologation-de-securite-en-neuf-etapes-simples>

16.2 Le Titulaire s'engage à appliquer les PES et ITE.

1. Objet du document

Ce document décrit les dispositions que <le prestataire d'externalisation> s'engage à mettre en oeuvre pour répondre aux exigences de sécurité de <le client>. Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d'externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en oeuvre.

Le candidat précisera le circuit d'approbation du Plan d'Assurance Sécurité, ses modalités d'application et l'étendue de sa diffusion.

2. Documents de référence

Ce paragraphe liste les documents de référence pour le Plan d'Assurance Sécurité.

À titre d'exemple, les documents applicables peuvent être les suivants :

- *le contrat ;*
- *le cahier des charges, incluant les exigences de sécurité du client ;*
- *le plan d'assurance qualité ;*
- *etc.*

3. Description du système externalisé

Ce paragraphe présente succinctement le système faisant l'objet de l'opération d'externalisation. L'accent sera mis sur les points qui justifient la mise en oeuvre de mesures de sécurité.

4. Rappel des exigences

Le candidat rappellera les exigences de sécurité du client ou fera référence au document les spécifiant.

5. Organisation

Le candidat indiquera l'organisation qu'il propose pour gérer la sécurité dans le projet d'externalisation.

On y trouve au minimum :

- le maître d'ouvrage agissant en tant que client ;
- le prestataire d'externalisation.

Si des co-traitants, sous-traitants ou fournisseurs peuvent intervenir directement, il indiquera leur rôle et précisera éventuellement les modalités de leur participation à la gestion de la sécurité du projet.

Il décrira l'organisation mise en place pour assurer les relations avec le maître d'ouvrage concernant les aspects sécurité :

- comité de suivi de la sécurité : fréquence, participants, modalités, périmètre du suivi ;
- organisation de la maîtrise d'ouvrage : responsable sécurité, rôle et moyens ; intervenants techniques ;
- organisation du prestataire : responsable sécurité, rôle et moyens ; responsables techniques, implication des co-traitants et sous-traitants éventuels ;
- diffusion du Plan d'assurance sécurité et des documents de suivi ;
- audits, contrôles réalisés par la maîtrise d'ouvrage ou à la demande de celle-ci : modalités, périmètre, exploitation des résultats.

Organisation de la maîtrise d'œuvre :

En tant que maître d'œuvre, <le prestataire d'externalisation> désignera un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité. Il est rattaché directement au responsable de l'opération, au directeur de projet par exemple, désigné par le <prestataire d'externalisation>.

Le responsable de la sécurité désigné par <le prestataire d'externalisation> prend en charge l'organisation des comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes-rendus [cf clause Comité de suivi].

Il pourra convier à ces réunions les intervenants impliqués dans les sujets inscrits à l'ordre du jour : sécurité applicative, sécurité des serveurs, sécurité des échanges...

Il conseille le client dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

Organisation de la maîtrise d'ouvrage :

<Le client> désignera un interlocuteur responsable de la sécurité du projet <projet d'externalisation>. Cet interlocuteur unique sera rattaché directement au directeur de projet. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour <le client>, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec le prestataire d'externalisation.

Des réunions de pilotage sécurité seront programmées tous les <période à évaluer>. Les participants à ces réunions pour <le client> seront le directeur du projet, le responsable de la sécurité, <liste à compléter> ainsi que le responsable technique ou fonctionnel lorsqu'ils sont impliqués dans les points à l'ordre du jour.

La sécurité globale de <l'opération d'externalisation> repose sur la participation active des différents intervenants : personnel interne qui avait un rôle dans le fonctionnement antérieur du système ou service faisant l'objet de l'opération d'externalisation [intégrateur, développeur, administrateur, exploitant, responsable technique, etc.], maîtrise d'ouvrage et maître d'œuvre.

Le responsable de la sécurité désigné par <le client> a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité lié à l'opération d'externalisation : politique de sécurité interne du <client>, documentation technique du système [documents d'ingénierie, documents d'exploitation, etc.], spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par le prestataire d'externalisation.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

6. Responsabilités liées au PAS

Le candidat, au travers de son responsable de la sécurité désigné, est responsable de la rédaction, de l'évolution et de l'application du Plan d'Assurance Sécurité.

Il s'applique à l'ensemble des équipes de la maîtrise d'œuvre (et aux sous-traitants éventuels).

Sa rédaction relève du responsable sécurité désigné par <le prestataire d'externalisation>. Il doit être approuvé par la maîtrise d'ouvrage ; sa bonne exécution est de la responsabilité du <prestataire d'externalisation> en tant que maître d'œuvre.

La cohérence de l'ensemble des mesures pourra être analysée et réévaluée lors des réunions d'avancement (ou revues de pilotage).

7. Procédure d'évolution du PAS

Le titulaire est responsable de la rédaction du PAS initial et de ses évolutions pour répondre aux exigences de sécurité du donneur d'ordres pendant toute la durée du contrat.

Voici une liste (non exhaustive) des situations susceptibles d'entraîner une modification du PAS :

- évolution du système d'information (configuration logicielle ou matérielle) ;
- évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- évolution du périmètre de l'opération.

En cas d'évolution du système, de son environnement, ou du périmètre de l'opération d'externalisation, le titulaire vérifie si le PAS doit être modifié. Si tel est le cas, il propose une modification au client. Si cette modification est acceptée, le PAS est révisé et soumis au client pour validation formelle.

Le responsable sécurité désigné par <le prestataire d'externalisation> est responsable de la rédaction du Plan d'Assurance Sécurité initial et de ses évolutions.

Une révision du Plan d'Assurance Sécurité pourra être réalisée en cas d'évolution du périmètre de l'opération ou des exigences de la maîtrise d'ouvrage, après accord de la maîtrise d'œuvre. Cette révision sera réalisée par le responsable sécurité désigné par <le prestataire d'externalisation>. La version révisée du PAS sera transmise à la maîtrise d'ouvrage pour validation, et diffusée à l'ensemble des acteurs pour application.

8. Applicabilité du PAS

L'applicabilité du PAS s'articule autour des trois points suivants :

- quelles sont les procédures à suivre lors de non respect du PAS ?
- quelle est la procédure à suivre pour une demande de dérogation ?
- quelles sont les pénalités encourues ?

Le Plan d'Assurance Sécurité est applicable à l'ensemble des acteurs du projet, au même titre que le Plan d'Assurance Qualité et avec la même priorité.

Un acteur du projet identifiant un non respect du PAS dans ses procédures et mesures doit en référer immédiatement au <prestataire d'externalisation>, qui en avertira la maîtrise d'ouvrage. Un modèle type de rapport de non respect sera annexé au PAS définitif, spécifiant la forme du rapport, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la clause de non respect.

Si la cause du non respect n'est pas corrigée dans un délai de <délai à estimer>, <le prestataire d'externalisation> subira une pénalité suivant la formule : <formule à calculer>.

Un acteur du projet n'étant pas à même de remplir l'ensemble des clauses du PAS devra effectuer une demande de dérogation auprès du <prestataire d'externalisation>, qui négociera avec <le client> l'ensemble des demandes de dérogation. Un modèle type de demande de dérogation sera annexé au PAS définitif, spécifiant la forme de la demande, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la demande de dérogation.

9. Mesures de sécurité

Le candidat décrira les mesures destinées à assurer la sécurité du système cible de l'opération d'externalisation pendant les différentes phases contractuelles : phase de transfert, phase d'exploitation, phase de réversibilité ou fin de contrat.

9.1 Transfert

Le candidat présentera dans ce paragraphe les mesures proposées pour sécuriser la phase de transfert du système (transfert de matériels ou de logiciels dans un projet d'externalisation) [cf *clause de transfert*].

Il décrira les procédures de contrôle de la sécurité du transfert mises en œuvre et identifiera ses obligations de *reporting* au comité de suivi sécurité [cf *clause de contrôle des prestations et des résultats*].

Les exigences de sécurité formulées par le client indiquent le niveau de confidentialité maximum des informations manipulées notamment lors du transfert. Une liste de personnes susceptibles de participer au transfert pourra être rédigée et communiquée au client. Le client devra indiquer s'il juge nécessaire que le personnel soit soumis à une clause de confidentialité ou procéder à une habilitation [cf *clause de confidentialité*].

9.2 Exploitation

Le candidat présentera dans ce paragraphe les mesures mises en place pour assurer la protection du système externalisé en réponse aux exigences identifiées par le client.

9.3. Réversibilité

Le candidat s'engagera à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le client, ou par un autre prestataire de service [cf *clause de réversibilité*].

10. Matrice de couverture des exigences de sécurité

Le candidat présentera les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences du donneur d'ordres. Il pourra pour ce faire reprendre dans un tableau les exigences énoncées, et lister la ou les mesure(s) répondant à chaque exigence.

11. Documentation de suivi

Le candidat recensera dans ce paragraphe l'ensemble de la documentation concernant la sécurité qu'il s'engage à fournir au titre du projet. Ces documents pourront être les suivants :

Nature du document :

Plan d'Assurance Sécurité, version 1

Plan d'Assurance Sécurité, version définitive

Dossier de sécurité

Plan de secours

Plan de gestion des incidents

Comptes-rendus de réunion du comité de suivi

Date de remise :

Remise du dossier de réponse à consultation

Début de phase de transfert

Début de phase d'exploitation

Début de phase d'exploitation

Début de phase d'exploitation

Une semaine après chaque réunion