

Sécurité

Annexe

- **EPELFI** - Etablissement Public d'Exploitation du Livre Foncier Informatisé
- 2a, rue de l'Artisanat - 67700 SAVERNE - Siret 130 004 633 00017 - APE 8411Z
- <http://www.livrefoncier.fr> - Tél. : +33 (0) 3 88 01 83 20 - Fax : +33 (0) 3 88 01 83 29

Sommaire

Annexe Sécurité	3
1. Clauses de sécurité	3
1.1. Responsabilité	3
1.2. Obligations du prestataire.....	3
1.3. Comité de suivi.....	3
1.4. Confidentialité.....	3
1.5. Localisation des données	4
1.6. Audits de sécurité.....	4
1.7. Application des plans gouvernementaux.....	4
1.8. Echanges de données et intériorisation dans le S.I. du client	4
1.9. Gestion des évolutions	4
1.10. Réversibilité.....	4
1.11. Résiliation	4
2. Exigences de sécurité.....	5
2.1. Gestion de la sécurité.....	5
2.2. Protection antivirale.....	5
2.3. Mises à jour, correctifs de sécurité	5
2.4. Sauvegardes et restauration	5
2.5. Continuité d'activité.....	5
2.6. Authentification	6
2.7. Confidentialité et intégrité des flux.....	6
2.8. Personnels en charge des prestations.....	6
2.9. Surveillance et contrôle des accès aux locaux du prestataire.....	7
2.10. Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles).....	7
3. Modèle de Plan d'Assurance Sécurité	8
3.1. Objet du document	8
3.2. Documents de référence.....	8
3.3. Description du système externalisé	8
3.4. Rappel des exigences	8
3.5. Organisation	8
3.6. Responsabilités liées au PAS	10
3.7. Procédure d'évolution du PAS	10
3.8. Applicabilité du PAS	10
3.9. Mesures de sécurité	11

Annexe Sécurité

1. Clauses de sécurité

1.1. Responsabilité

Voir CCAP.

1.2. Obligations du prestataire

Le prestataire 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 client des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le prestataire informera préalablement le client de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

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 prises en compte.

1.3. Comité de suivi

Le prestataire aura l'obligation de participer au comité de suivi de la maintenance applicative qui outre les aspects fonctionnels traitera :

- de la validation des évolutions du plan assurance sécurité
- des questions techniques touchant à la sécurité : collaboration dans la gestion des droits et la gestion des incidents
- des préconisations d'améliorations, exploitation des résultats des audits de contrôle
- des prestations sécurité
- des obligations liées à la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés : déclaration par le client auprès de la CNIL, communication des déclarations au prestataire, informations par le prestataire des modalités de gestion ou d'exploitation des applications et des modifications de celles-ci.
- des conditions techniques et financières de transfert des moyens de sécurité matériels et logiciels mis en place, en cas de réversibilité de l'opération. Des réunions périodiques seront planifiées contractuellement

1.4. Confidentialité

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

1.5. Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles.

Le prestataire doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.).

1.6. Audits de sécurité

L'EPELFI pourra à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire. Les audits pourront être réalisés par le client, ou délégués à un tiers. Le contrôle pourra comprendre visite des locaux du prestataire, entrevues individuelles des membres des équipes, accès aux machines mises à la disposition.

L'audit sera notifié au prestataire avec 15 jours de préavis.

1.7. Application des plans gouvernementaux

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 d'information et réseaux de télécommunications des opérateurs d'infrastructures vitales.

Dans le cadre de ce marché, le prestataire pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par le donneur d'ordres. Ces mesures sont susceptibles d'évoluer. Les modifications seront régulièrement transmises durant l'exécution du marché.

1.8. Echanges de données et interiorisation dans le S.I. du client

Le logiciel retenu nécessitera des échanges de données avec le reste du système d'information du client. Ces échanges seront formalisés au moyen d'une matrice de flux. Tous les flux seront cryptés par le logiciel ou via un accès dédié.

1.9. Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité. En cas d'évolution, le prestataire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

1.10. Réversibilité

Voir CCTP.

1.11. Résiliation

Voir CCAP.

2. Exigences de sécurité

2.1. Gestion de la sécurité

Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité de ses infrastructures d'hébergement. Cette description peut être avantageusement présentée selon les 4 étapes de la méthode de gestion de la qualité PDCA (*Plan-Do-Check-Act*) :

- phase de préparation ;
- phase de réalisation ;
- phase de vérification : préciser la fréquence ainsi que le périmètre technique et organisationnel des audits réalisés en interne par les équipes du prestataire ou par une société tierce ;
- phase d'ajustement (mesures correctives suite aux insuffisances constatées lors de la vérification).

2.2. Protection antivirale

Pour les machines qui le nécessitent, une politique antivirale stricte devra être mise en place. La mise à jour des signatures devra être automatique et d'une fréquence élevée (30 minutes).

La politique antivirale appliquée sur le système d'information du titulaire devra être précisée. Le candidat fournira dans sa réponse une description des solutions anti-virus sur lesquelles se base son service de messagerie (logiciel, version) et décrira les modalités et la fréquence de mise à jour du service.

2.3. Mises à jour, correctifs de sécurité

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

2.4. Sauvegardes et restauration

Le titulaire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé.

2.5. Continuité d'activité

Le candidat indiquera les mesures techniques, organisationnelles, procédurales qu'il s'engage à prendre pour assurer la continuité de ses activités, ou en cas de sinistre la reprise d'activité conformément aux exigences définies dans la clause sur la convention de service.

Les procédures de sauvegarde et de secours seront auditées conformément aux modalités identifiées dans la clause relative aux audits de sécurité.

2.6. Authentification

Pour chaque interface d'accès à sa plateforme de maintenance le titulaire doit fournir une documentation précisant :

- 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.

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).

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 candidat présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité.

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

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

Les mots de passe doivent satisfaire aux contraintes de complexité suivantes :

- Avoir une longueur minimale de 10 caractères (sauf limitation technique) ;
- Comporter au minimum une majuscule, un chiffre et un caractère spécial ;
- Ne pas être vulnérables aux attaques par dictionnaire.

2.7. Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH SSL, Ipsec,etc.), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties. Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière. Le candidat indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

2.8. Personnels en charge des prestations

Le titulaire s'engage à fournir une liste, régulièrement mise à jour, des personnels autorisés à intervenir sur la maintenance du S.I. AMALFI.

Le candidat précisera les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Si le candidat ou des employés de son entreprise possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention.

Le candidat précisera dans son offre si d'autres clients peuvent accéder aux mêmes locaux que ceux utilisés par le maître d'ouvrage et dans quelle mesure il sera possible de limiter ces accès à la demande de ce dernier.

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer un renforcement des contrôles d'accès physiques et logiques à ces équipements.

2.9. Surveillance et contrôle des accès aux locaux du prestataire

Le titulaire doit mettre en œuvre un dispositif permettant de réserver l'accès aux locaux hébergeant l'ensemble des machines et postes de travail utilisés aux seules personnes autorisées par le client : filtrage des accès au bâtiment ou aux étages, et filtrage des accès aux salles machines.

Le candidat doit détailler tous les moyens mis en œuvre afin d'assurer la sécurité des locaux notamment :

- moyens de surveillance, dispositifs anti-intrusion ;
- contrôle et enregistrement des accès (gardiennage, sas, moyen d'identification, etc.) ;
- protection physique des équipements (verrouillage des baies, etc.).

2.10. Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles)

Les intervenants des sociétés assurant la maintenance ou le support technique de solutions doivent être accompagnés par une personne habilitée à intervenir sur le système pendant toute la durée de leur intervention. Si un intervenant a besoin de se connecter au système, il doit utiliser un compte spécifique permettant de garantir l'imputabilité de ses actions.

Le candidat présentera les mesures techniques et organisationnelles pour empêcher les extractions massives d'information (par exemple : extraction d'une copie de la base de données à partir d'un poste).

Les supports de stockage de données (disques durs, bandes de sauvegardes, etc.) restent la propriété du client. Ils ne peuvent être mis au rebut ou emportés par une société de maintenance, ou encore réutilisés à d'autres fins que celles prévues initialement sans l'autorisation expresse du donneur d'ordres.

Ils doivent être conservés en lieu sûr par le titulaire, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée. L'effacement ou la destruction ont lieu en présence d'un représentant du donneur d'ordres.

3. Modèle de Plan d'Assurance Sécurité

Le plan-type proposé ci-après pourra être joint à l'appel d'offres comme base de rédaction du Plan d'Assurance Sécurité qui sera fourni par les candidats en réponse à la consultation.

Les paragraphes en italique constituent des propositions de contenu du Plan d'Assurance Sécurité à fournir par le prestataire d'externalisation.

3.1. Objet du document

Ce document décrit les dispositions que <le prestataire d'externalisation> s'engage à mettre en œuvre 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 œuvre.

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

3.2. 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.*

3.3. 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 œuvre de mesures de sécurité.

3.4. Rappel des exigences

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

3.5. 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 cotraitants, 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 cotraitants 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.

3.6. 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).

3.7. 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.

3.8. 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.

3.9. 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.

3.9.1. 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]*.

3.9.2. 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.

3.9.3. 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]*.

3.9.4. 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.

3.9.5. 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 :

<i>Nature du document</i>	<i>Date de remise</i>
Plan d'Assurance Sécurité, version 1	Remise du dossier de réponse à consultation
Plan d'Assurance Sécurité, version définitive	Début de phase de transition
Dossier de sécurité	Début de phase d'exécution
Plan de secours	Début de phase d'exécution
Plan de gestion des incidents	Début de phase d'exécution