

Exigences de Sécurité des Systèmes d'Information (SSI) pour les candidats ou titulaires de l'EFS

SC2965

FOURNITURE DE SEPARATEURS D'APHERESE POUR LA PRODUCTION DE CPA DESTINE A LA VIRO ATTENUATION ET PLASMA SECONDAIRE, DMU ET PRESTATIONS ASSOCIEES

HISTORIQUE DES VERSIONS

VERSION	DATE	OBSERVATIONS	REDACTEUR	VERIFICATEUR	APPROBATEUR
1.0	21/07/2021	Création du document	Maricela Pélegrin-Bomel RNSSI		
3.1	27/05/2025	Ajout des précisions sur la Plan d'Assurance Sécurité	Maricela Pélegrin-Bomel RNSSI		

SOMMAIRE

1.	INTRODUCTION	4
2.	SECURITE ORGANISATIONNELLE	5
3.	SECURITE INFORMATIQUE	5
3.1.	SPECIFICITES POUR LES AUTOMATES	5

3.2.	SPECIFICITES POUR LE DEVELOPPEMENT INFORMATIQUE	6
4.	MAINTENANCE	8
5.	TELEMAINTENANCE AUTOMATES	9
5.1.	GENERALITES	9
5.2.	MAINTENANCE SUR SITE	10
5.3.	TELEMAINTENANCE	10
5.4.	MAINTENANCE PREDICTIVE	10
6.	FOURNITURE DE SERVICE SAAS (SOFTWARE AS A SERVICE)	11
6.1.	GENERALITES	11
6.2.	GESTION DES ACTIFS	11
6.3.	CONTROLE D'ACCES ET GESTION DES IDENTITES	11
6.3.1.	Contrôle d'accès	11
6.4.	CRYPTOLOGIE	12
6.5.	SECURITE DE L'EXPLOITATION	13
6.6.	INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION	14
6.7.	LOCALISATION DES DONNEES	14
7.	RELATIONS AVEC LES TIERS	14
8.	FIN DU CONTRAT	15
9.	PLAN DE CONTINUITE D'ACTIVITE	15
10.	PLAN D'ASSURANCE SECURITE (PAS)	15
11.	AUDITS DE SECURITE	15
	ANNEXE 1 : MATRICE DE CONFORMITE	17

GLOSSAIRE :

AES	<i>Advanced Encryption Standard</i>
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
APSAD	Assemblée Plénière des Sociétés d'Assurance Dommage
EFS	Etablissement Français du Sang
PAS	Plan d'Assurance Sécurité

PCA	Plan de Continuité d'Activité
Prescripteur	Client Interne de l'EFS
RGS	Référentiel Général de Sécurité
RGPD	Le règlement général sur la protection des données
RNSSI	Responsable National de la Sécurité des Systèmes d'Information
SAAS	<i>Software as a service</i> ¹ (Logiciel en tant que service)
SI	Systèmes d'Information
SSI	Sécurité des Systèmes d'Information

1. INTRODUCTION

L'Etablissement Français du Sang (EFS), est conscient de sa mission en tant qu'opérateur unique de la transfusion sanguine en France mais aussi de son obligation de protéger les données personnelles de ses donneurs, les receveurs et de son personnel.

A ce titre, l'EFS doit assurer la continuité de la transfusion sanguine en France et se doit de vérifier que les activités confiées à des tiers partenaires ou à des sous-traitants se déroulent dans le respect des conditions de disponibilité, intégrité et confidentialité fiabilité et authentification imposées par les obligations légales de son activité dépendante de son système d'information.

¹ Ce service concerne la mise à disposition par le candidat ou titulaire d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le candidat ou titulaire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application

Le présent document comporte les exigences de Sécurité des Systèmes d'Information de l'EFS applicables aux prestations prévues au marché. Les volets relatifs à la sécurité organisationnelle, la sécurité physique des locaux, la sécurité informatique, les exigences SaaS, la télémaintenance, la relations avec les tiers et le plan de continuité d'activité y sont présentés.

Le candidats et/ou titulaire sont invités à prendre connaissance des mesures de sécurité indiquées et à y apporter une réponse dans le cadre de réponse relatif aux exigences SSI annexée au présent document (Matrice de conformité). Cette réponse fera l'objet d'une analyse afin de déterminer la conformité ou non du candidat à chacune des exigences et sera notée sur la base du critère prévu au règlement de la consultation.

Le candidat et/ou titulaire doit garder à l'esprit que la non-conformité n'est pas un blocage pour devenir le titulaire et participer à cette consultation. Le titulaire aura le temps nécessaire pour attendre la conformité et sera guidé, en cas de besoin pour l'atteindre.

Le tableau ci-dessous doit vous guider pour la réponse aux exigences en vous précisant le résultat recherché sur chaque grand domaine des exigences.

DOMAINE	OBJECTIF/RESULTAT RECHERCHE
Sécurité Organisationnelle	Réponse obligatoire pour tout type de prestation. L'objectif est de savoir comment la sécurité est intégrée à votre organisation et fonctionne dans votre entreprise. De plus, l'EFS souhaite avoir une idée représentative des moyens mis en œuvre.
Sécurité Informatique	Réponse obligatoire pour les prestations de développement informatique, exploitation de service ou toute autre prestation nécessitant une connexion au système d'information de l'EFS. Ces exigences doivent être intégrées dès les premières étapes de la conception et développement et être appliquées tout au long du cycle de vie des systèmes pour garantir une sécurité robuste et durable face aux menaces en constante évolution. Les exigences de ce domaine sont valables dans le cas d'une prestation de développement pour le produit livré dans le cadre de cette prestation.
Maintenance	Réponse obligatoire. Les exigences de cette partie concernent la maintenance du matériel et du logiciel qui s'y rattache et concerne les applications utilisateurs.
Télémaintenance automates	Réponse obligatoire. Les exigences de cette partie concernent la maintenance du matériel et du logiciel qui s'y rattache et ne concerne pas les applications utilisateurs.
Exigences des prestations SaaS	Obligation de réponse pour toute prestation dans le Cloud de type <i>Software as a Service</i> sauf pour un candidat ou titulaire ayant le visa SecNumCloud et/ou Cloud de Confiance de l'ANSSI. Le candidat ou titulaire devra répondre aux exigences organisationnelle, physique, plan de continuité d'activité et plan d'assurance sécurité.
Relations avec les tiers	Obligation de réponse dans le cadre d'intervention de tout sous-traitant. Ce dernier doit appliquer et respecter nos exigences de sécurité des systèmes d'information.
Plan de Continuité d'Activité	Obligation de réponse pour toute prestation d'exploitation et/ou de service.
Plan d'Assurance Sécurité	Obligation de réponse uniquement si le candidat devient le Candidat du service

En réponse à nos exigences il est impératif de :

- Les intégrer dans la conception et/ou réalisation des produits ou prestations ;
- Remplir la matrice de conformité jointe en annexe des exigences.

Pour toute question complémentaire, nous restons à votre entière disposition selon les conditions indiquées dans les prestations prévues au marché.

2. SECURITE ORGANISATIONNELLE

SECORG1 : Le candidat ou titulaire doit présenter une politique de sécurité formalisée dont le périmètre couvre les risques de continuité de service et de malveillance auxquels il est exposé au titre de la prestation.

SECORG2 : L'organisation du candidat ou titulaire doit comprendre au moins un responsable sécurité pour l'ensemble des domaines concourant au bon déroulement de la prestation.

SECORG3 : Les moyens mis à disposition des responsables sécurité doivent leur permettre de faire appliquer la politique de sécurité.

SECORG4 : Tout collaborateur du candidat ou titulaire participant à l'activité de l'EFS doit respecter les procédures et les règles de sécurité applicables dans le cadre de la réalisation de la prestation.

SECORG5 : Tout collaborateur du candidat ou titulaire participant à l'activité de l'EFS doit avoir signé un engagement personnel de confidentialité dans le cadre de son contrat de travail.

SECORG6 : Le candidat ou titulaire doit documenter et mettre en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.

SECORG7 : Le candidat ou titulaire doit sensibiliser à la sécurité de l'information et aux risques liés à la protection des données l'ensemble des personnes impliquées dans la fourniture du service.

SECORG8 : Le candidat ou titulaire doit obligatoirement faire appliquer les exigences de sécurité à l'ensemble des sous-traitants participant à la délivrance du service.

SECORG9 : Le candidat doit documenter et mettre en œuvre un plan de formation concernant la sécurité de l'information adapté au service et aux missions des personnels. Le responsable de la sécurité des systèmes d'information du prestataire doit valider formellement le plan de formation concernant la sécurité de l'information

3. SECURITE INFORMATIQUE

3.1. SPECIFICITES POUR LES AUTOMATES

SECINF-AUTOM1 : La fonction « *autorun* » d'exécution automatique sur les périphériques amovibles est désactivée sur l'équipement. Ceci afin de garder le contrôle de ces médias externes et de réduire ainsi le risque d'exécution de codes malveillants susceptible d'infecter l'équipement biomédical.

SECINF-AUTOM2 : La connexion au système analytique d'un support de stockage externe à des fins de mise à jour applicative, lors d'une intervention sur site ne doit être réalisée qu'après que le titulaire ait effectué une analyse complète du media sur un poste de l'établissement doté d'un progiciel antivirus

à jour au niveau de ses bases de signatures. Cette procédure est partie intégrante des procédures de maintenance sur site.

SECINF-AUTOM3 : Préalablement à la réalisation d'une opération de maintenance ou télémaintenance, le tiers s'engage à informer le Représentant des pouvoirs adjudicateurs (RPA) de la date, de la durée et de la nature des interventions, ainsi que du nom de l'intervenant. Le RPA valide les demandes et informe le tiers des plages horaires autorisées pour l'intervention.

A la notification le titulaire précisera le nom, les fonctions et les coordonnées des intervenants qui seront habilités à demander un accès à distance pour réaliser les opérations de télémaintenance. Cette liste devra être mise à jour autant que de besoins.

SECINF-AUTOM4 : Les accès à distance pour la télémaintenance doivent être réalisés uniquement via la solution homologuée par l'établissement (WALLIX), suite à une demande explicite de la part du tiers précisant l'objet de l'intervention. L'accès est autorisé uniquement pendant la plage horaire d'intervention préalablement communiquée au RPA.

Des rapports d'intervention de maintenance et télémaintenance doivent être fournis par les tiers au RPA après chaque opération. Ils doivent décliner la raison et la nature de l'intervention réalisée, les intervenants impliqués, la durée de l'opération et les résultats obtenus.

SECINF-AUTOM5 : Le candidat ou titulaire s'engage à utiliser les systèmes d'information et/ou informatiques de l'EFS (applications, système, réseaux, etc.) uniquement dans le cadre de l'exécution des prestations définies et contractualisées. Il le fait en respectant les exigences de sécurité relatives à la (télé)maintenance sur les automates de l'EFS indiquées dans ces exigences.

SECINF-AUTOM6 : Le candidat ou titulaire s'engage à l'application des correctifs critiques (Patches) du système d'exploitation permettant d'utiliser la version supportée par l'éditeur de ce dernier. Soit la mise à jour est faite par le Titulaire, soit, à défaut, par l'établissement qui applique ces correctifs, après information de celui-ci qui doit alors signaler toute incompatibilité entre les correctifs et l'équipement.

Dans ce cas, le candidat ou titulaire s'engage à proposer rapidement une solution corrective ou de contournement. La mise à niveau des correctifs est prévue usuellement sur une base mensuelle ; une procédure d'application de correctifs en urgence est prévue. Le Titulaire s'engage à fournir un système d'exploitation dont le support est toujours assuré par l'éditeur.

SECINF-AUTOM7 : Une matrice des flux réseau est communiquée par le candidat ou titulaire. Elle précise la nature des échanges, les ports et protocoles nécessaires à ces échanges. Cette matrice permet à l'établissement d'identifier précisément les flux liés à l'équipement et de configurer les équipements d'interconnexion de manière à n'autoriser que les flux nécessaires et filtrer ainsi les autres. La matrice des flux est conforme au format ci-dessous.

Nature de l'information – finalité de l'échange	Adresse source	Port source (Indiquer dynamique si c'est le cas)	Adresse cible	Port cible	Protocole de communication	Volumétrie (bande passante)

3.2. SPECIFICITES POUR LE DEVELOPPEMENT INFORMATIQUE

SECDEV-GESTIDEN1 : Pour la gestion des identités et des accès, le candidat ou titulaire doit s'assurer que seules les bonnes personnes peuvent accéder au système et aux données.

SECDEV-GESTIDEN2 : Pour la gestion des identités il doit aussi mettre en place une authentification forte et gérer les permissions d'accès aux systèmes.

SECDEV-AUTHENCENTRALE : le candidat ou titulaire doit utiliser des technologies standardisées comme LDAP, OAuth ou SSO pour gérer l'accès à plusieurs systèmes de manière cohérente et sécurisée et assurer une authentification centralisée

SECDEV-CHIFFREDATA1 : Pour le chiffrement des données, le candidat ou titulaire doit rendre les données illisibles pour toute personne non autorisée. Il doit également utiliser des mécanismes de chiffrement pour les données en transit et au repos ; ainsi que protéger les données envoyées sur Internet avec des connexions sécurisées.

SECDEV-CHIFFREDATA2 : Dans la suite du chiffrement des données, le candidat ou titulaire doit ainsi stocker les informations sensibles sous forme chiffrée.

SECDEV-JOURNAUX 1 : Pour les journaux et suivi des activités, le candidat ou titulaire doit Implémenter des journaux d'audit pour détecter et analyser les changements non autorisés. Ainsi, il doit garder la trace des actions importantes pour détecter les problèmes ou abus afin de pouvoir obtenir les informations sur les actions sensibles telles que ;

- Les connexions ;
- Les modifications de données ;
- Les erreurs ou les comportements inhabituels ;
- Voir les modifications ou la suppression des journaux.

SECDEV- PROTECAPPLI1 : Concernant la sécurisation de l'application, le candidat ou titulaire doit s'assurer que le système fonctionne comme prévu, sans permettre de mauvaises utilisations. Il doit aussi s'assurer qu'un utilisateur malveillant n'envoie pas des informations dangereuses.

SECDEV- PROTECAPPLI 2 : Le candidat ou titulaire doit donner par ailleurs un minimum d'autorisations aux composants du système pour limiter les dégâts en cas de problème et surtout effectuer une séparation des environnements de test et de production.

SECDEV-PROTECDATASEN : Pour la protection des données sensibles, le candidat ou titulaire doit limiter l'accès aux données de ce type uniquement aux personnes qui en ont besoin. Il doit dans la mesure du possible anonymiser les données sensibles.

SECDEV-SECUAPPLI : Pour la protection des applications contre les vulnérabilités et attaques courantes, le candidat ou titulaire, doit effectuer des tests d'intrusion réguliers et des analyses statiques ou dynamiques du code pour identifier et corriger les failles.

SECDEV-SECURISE : Pour le développement sécurisé, le candidat ou titulaire doit suivre les bonnes pratiques reconnues, comme les recommandations OWASP, pour prévenir les vulnérabilités des telles que les injections SQL ou les scripts intersites (XSS).

SECDEV-VALIDDATA ; Le candidat ou titulaire doit valider les données. Il doit contrôler systématiquement toutes les données saisies par les utilisateurs pour éviter les attaques par injection.

SECDEV-MOINDRE PRIV : Principes de moindre privilège. Le candidat ou titulaire doit limiter les droits d'accès au strict nécessaire pour chaque utilisateur ou processus.

SECDEV-BIBLIOEXT : Pour les dépendances et bibliothèques externes, le candidat ou titulaire doit s'assurer que les outils ou morceaux de code utilisés sont sûrs. Il doit maintenir les bibliothèques et frameworks à jour pour éviter les vulnérabilités connues.

SECDEV-SECU SRVRS : Quant à la sécurisation des serveurs et réseaux, le candidat ou titulaire doit protéger les machines qui hébergent le système et les connexions entre elles ainsi que limiter les connexions non autorisées

SECDEV-REAINCIDENTS : Pour la réaction aux incidents de sécurité, le candidat ou titulaire doit être en mesure de détecter et répondre rapidement en cas d'attaque ou de problème (panne importante ou piratage). Il doit prévoir des mécanismes de sauvegarde et de redondance. Et finalement mettre en œuvre des solutions contre les attaques par déni de service (DDoS).

SECDEV-VERSIONNING – Le candidat ou titulaire doit effectuer le contrôle des versions. Il doit mettre en œuvre des systèmes de versionnage permettant de suivre et restaurer les versions antérieures des fichiers ou des applications en cas de corruption.

SECDEV-REGLESNORMES : Concernant le respect des règles et normes, le candidat ou titulaire doit s'assurer que le système respecte les lois et bonnes pratiques (suivi des réglementations et méthodes de travail).

SECDEV-ANACODE : Pour l'analyse de code, le candidat ou titulaire doit effectuer des tests de sécurité pendant le cycle de développement (ex. : SAST, DAST).

SECDEV MAJ DEPEND : Pour la mise à jour des dépendances, le candidat ou titulaire doit maintenir les bibliothèques et frameworks à jour pour éviter les vulnérabilités connues.

SECDEV-TESTAUDITS : Pour les tests et audits réguliers, le candidat ou titulaire doit effectuer des tests de pénétration : et simuler des attaques pour identifier les failles.

SECDEV-AUDITCONFO : le candidat ou titulaires doit dans les aspects d'audits de conformité, de vérifier régulièrement que le SI respecte les politiques de sécurité définies par son entité

SECDEV-CRYPTO : Le candidat ou titulaire doit utiliser des protocoles sécurisés pour les communications réseaux TLS/SSL.

SECDEV-GESCLE : le candidat ou titulaire doit, dans la cadre de la gestion des clés, mettre en place une infrastructure de gestion des clés (KMS).

SECDEV-FORMSENS : Le candidat ou titulaire doit assurer la formation des développeurs aux pratiques de codage sécurisé. Il doit aussi faire en sorte que tout le monde dans son équipe comprenne l'importance de la sécurité.

SECDEV-ANALYSE : Le candidat ou titulaire doit faire effectuer des tests d'intrusion réguliers et des analyses statiques ou dynamiques du code pour identifier et corriger les failles.

SECDEV-SVGD HSITE : Sauvegardes hors site : Le candidat ou titulaire doit réaliser des copies régulières des données sur des sites géographiquement éloignés pour limiter les pertes.

4. MAINTENANCE

Dans le cadre du maintien de la sécurité de son système d'information, l'EFS exige le respect des règles ci-dessous dans le cadre des différentes opérations de maintenances/

MAINTEN1 : Si le titulaire propose un système de supervision destiné au maintien en condition opérationnelle et de sécurité du système d'information, il devra en décrire précisément les catégories de données transférées. La protection de ces dernières devra être encadrée.

MAINTEN2 : L'EFS interdit strictement toute récupération de Données à Caractère Personnel (DCP²) ou données de santé.

MAINTEN3 : Les données techniques (configuration des équipements) de l'EFS exploitées par les équipes de support chez le titulaire doivent être protégées et ne doivent pas être divulguées.

MAINTEN4 : Le candidat indiquera dans sa réponse où (pays, région, type d'hébergement) sont hébergées les données prélevées. Le candidat indiquera par ailleurs obligatoirement les certifications et habilitations de sécurité dont lui ou ses sous-traitants sont titulaires.

² Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.

MAINTEN5 : Au niveau des postes de travail standard de l'EFS, aucun outil de prise de contrôle à distance ne peut être installé ou exécuté. Le seul outil de prise de contrôle à distance autorisé est celui de l'EFS.

MAINTEN6 : Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (locaux, matériels, données, logiciels, habilitations), notamment mise à jour des correctifs de sécurité et dispositif de protection contre les codes malveillants.

MAINTEN7 : Il est de la responsabilité du titulaire de connaître en toutes circonstances les actions et l'identité de toute personne qui se connecte ou s'est connectée sur le SI de l'EFS et d'en assurer la traçabilité. Cette traçabilité devra être communiquée sur demande de l'EFS.

MAINTEN8 : Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées en application du principe de minimisation des données.

MAINTEN9 : Le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs fournis et met à disposition les correctifs et préventifs nécessaires dans les délais appropriés.

MAINTEN10 : Le titulaire s'engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du titulaire, la correction et la prise en charge des impacts à sa charge. Les résultats des tests pourront être communiqués sur demande à l'EFS.

MAINTEN11 : Selon les besoins d'intervention l'accès aux systèmes à maintenir ou exploiter sera ouvert et fermé par l'établissement l'EFS à la demande (du mainteneur ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance).

MAINTEN12 : Le titulaire doit informer la RNSSI de l'EFS de tout incident de sécurité concernant ses dispositifs connectés ou son SI pouvant impacter son matériel, le service ou les données de l'EFS. Le titulaire s'engage à mobiliser les ressources nécessaires pour assurer le traitement de l'incident de sécurité sur les dispositifs déployés dans l'EFS. Si l'incident concerne un traitement relatif au RGPD, les dispositions relatives au traitement des incidents s'appliqueront aussi.

5. TELEMAINTENANCE AUTOMATES

5.1. GENERALITES

Dans le cadre du maintien de la sécurité de son système d'information, l'EFS exige le respect des règles ci-dessous dans le cadre des différentes opérations de maintenances des automates biomédicaux dont il dispose ;

TELEMAIN1 : L'EFS interdit strictement toute récupération de Données à Caractère Personnel (DCP³) ou données de santé

TELEMAIN2 : Tout prélèvement de données, or DCP et données de santé devra être dûment justifié en indiquant précisément la nature des données et l'usage qui en sera fait. Sur la base de ces éléments, il fera l'objet d'une validation préalable par l'EFS.

TELEMAIN3 : Le candidat indiquera dans sa réponse où (pays, région, type d'hébergement) sont hébergées les données prélevées. Le candidat indiquera par ailleurs obligatoirement les certifications et habilitations de sécurité dont lui ou ses sous-traitants sont titulaires

³ Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.

5.2. MAINTENANCE SUR SITE

TELEMAIN4 : Toute clé USB destinée à être connectée sur un automate doit préalablement subir un contrôle antiviral réalisé par un agent de l'EFS.

5.3. TELEMAINTENANCE

TELEMAIN5 : Les accès en télémaintenance sont autorisés uniquement via les systèmes (réseau, VPN, prise en main à distance, etc...) validés par l'EFS.

TELEMAIN6 : La connexion de télémaintenance du titulaire doit se faire via un serveur sécurisée mise à disposition par l'EFS conformément à sa politique de sécurité.

TELEMAIN7 : Les accès en télémaintenance ne sont possibles qu'à la condition que les automates soient cloisonnés au niveau du réseau. Aucune exception à cette règle ne sera acceptée, même temporairement.

TELEMAIN8 : Tout accès fera l'objet d'une demande d'approbation par le métier au moment de la connexion par le tiers.

TELEMAIN9 : Tout accès sera tracé (horodatage de la connexion et des actions réalisées par le tiers).

TELEMAIN10 : Le formulaire d'habilitation transmis par l'EFS devra être dûment complété par le tiers avant la création d'un accès en télémaintenance.

TELEMAIN11 : Tout compte d'accès doit être nominatif et fera l'objet d'une fiche d'habilitation individuelle.

TELEMAIN12 : Le tiers s'engage à informer sans délai l'EFS en cas mouvement de personnel.

TELEMAIN13 : Lors de sa création, la date de validité d'un accès sera égale à la date de fin du contrat. A défaut, la durée sera positionnée à un (1) an.

TELEMAIN14 : Le tiers devra procéder à une revue d'habilitation annuelle des comptes actifs

TELEMAIN15 : L'EFS se réserve le droit de couper, sans préavis, son accès internet en cas de force majeure.

TELEMAIN16 : Tout accès à distance devra se solder par un compte-rendu d'intervention qui sera transmis par messagerie électronique sous 8 heures au demandeur à l'origine de la demande d'intervention.

TELEMAIN17 : L'accès distant ne sera permis que depuis des plages d'adresses IP déclarées par le télémainteneur.

5.4. MAINTENANCE PREDICTIVE

TELEMAIN18 : Toute demande de mise en place de maintenance prédictive devra faire l'objet d'une demande préalable détaillant, outre la nature des données (cf. point 2 des règles générales), la volumétrie et la fréquence des échanges

TELEMAIN19 : L'EFS se réserve le droit d'auditer le trafic entre l'automate et le serveur distant.

TELEMAIN20 : L'EFS se réserve le droit de couper, sans information préalable, l'accès sortant d'un automate en cas d'impact notable sur les performances et/ou la sécurité du réseau de l'EFS.

TELEMAIN21 : L'EFS se réserve le droit de couper son accès internet en cas de force majeure.

6. FOURNITURE DE SERVICE SAAS⁴ (SOFTWARE AS A SERVICE)

6.1. GENERALITES

Le prestataire mettra en œuvre les mesures de sécurité suivantes :

SAAS-GEN1 : Le prestataire doit faire signer la charte informatique à l'ensemble des personnes impliquées dans la fourniture du service.

SAAS-GEN2 : Dans la mesure où un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, le prestataire doit avertir le commanditaire et l'informer par écrit des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant

SAAS-GEN3 : Le prestataire doit, sur demande d'un commanditaire, lui rendre accessible le règlement intérieur et la charte d'éthique. Le commanditaire doit la rendre accessible ensuite à la RNSSI de l'EFS

6.2. GESTION DES ACTIFS

SAAS-GESACT1 : Lorsque le commanditaire confie au prestataire des données soumises à des contraintes légales ou réglementaires, le prestataire doit identifier les besoins de sécurité spécifiques associés à ces contraintes.

SAAS-GESACT2 : Il est recommandé que le prestataire documente et mette en œuvre une procédure pour le marquage et la manipulation de toutes les informations participant à la délivrance du service, conformément à son besoin de sécurité défini à l'exigence précédente.

SAAS-GESACT3 : Lorsque des supports amovibles sont utilisés sur l'infrastructure technique ou pour des tâches d'administration, ces supports doivent être dédiés à un usage.

6.3. CONTROLE D'ACCES ET GESTION DES IDENTITES

6.3.1. CONTROLE D'ACCES

SAAS-CTLACC1 : Le candidat ou titulaire doit réviser annuellement la politique de contrôle d'accès et à chaque changement majeur pouvant avoir un impact sur le service.

SAAS-CTLACC2 : Le candidat ou titulaire doit documenter et mettre en œuvre une procédure d'enregistrement et de désinscription des utilisateurs s'appuyant sur une interface de gestion des comptes et des droits d'accès. Cette procédure doit indiquer quelles données doivent être supprimées au départ d'un utilisateur.

SAAS-CTLACC3 : Le candidat ou titulaire doit documenter et mettre en œuvre une procédure permettant d'assurer l'attribution, la modification et le retrait de droits d'accès aux ressources du système d'information du service.

SAAS-CTLACC4 : Le candidat ou titulaire doit tenir à jour l'inventaire des utilisateurs sous sa responsabilité disposant de droits d'administration sur les ressources du système d'information du service.

⁴ Ce service concerne la mise à disposition par le candidat ou titulaire d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le candidat ou titulaire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application

SAAS-CTLACC5 ; Le candidat ou titulaire doit être en mesure de fournir, pour une ressource donnée mettant en œuvre le service, la liste de tous les utilisateurs y ayant accès, qu'ils soient sous la responsabilité du candidat ou titulaire ou du commanditaire ainsi que les droits d'accès qui leurs ont été attribué.

SAAS-CTLACC6 : Le candidat ou titulaire doit être en mesure de fournir, pour un utilisateur donné, qu'ils soient sous la responsabilité du candidat ou titulaire ou du commanditaire, la liste de tous ses droits d'accès sur les différents éléments du système d'information du service.

SAAS-CTLACC7 : Le candidat ou titulaire doit proposer au commanditaire des moyens d'authentification à multiples facteurs pour l'accès des utilisateurs finaux.

SAAS-CTLACC8 : Lorsque des comptes techniques, non nominatifs, sont nécessaires, le candidat ou titulaire doit mettre en place des mesures obligeant les utilisateurs à s'authentifier avec leur compte nominatif avant de pouvoir accéder à ces comptes techniques.

SAAS-CTLACC9 : Les comptes d'administration sous la responsabilité du candidat ou titulaire doivent être gérés à l'aide d'outils et d'annuaires distincts de ceux utilisés pour la gestion des comptes utilisateurs placés sous la responsabilité du commanditaire.

SAAS-CTLACC10 : Les interfaces d'administration utilisées par le candidat ou titulaire ne doivent pas être accessibles à partir d'un réseau public et ainsi ne doivent permettre aucune connexion des utilisateurs sous la responsabilité du commanditaire.

SAAS-CTLACC11 : Si des interfaces d'administration sont mises à disposition du commanditaire avec un accès via un réseau public, les flux d'administration doivent être authentifiés et chiffrés avec des moyens en accord avec les exigences du chapitre Cryptologie.

SAAS-CTLACC12 : Le candidat ou titulaire doit mettre en place un système d'authentification à double facteur pour l'accès : aux interfaces d'administration utilisées par le candidat ou titulaire et aux interfaces d'administration dédiées aux commanditaires.

SAAS-CTLACC13 : Les interfaces d'administration mises à disposition des commanditaires doivent être différenciées des interfaces permettant l'accès des utilisateurs finaux.

SAAS-CTLACC14 : Le candidat ou titulaire doit mettre en œuvre des mesures de cloisonnement appropriées entre ses commanditaires.

SAAS-CTLACC15 : Le candidat ou titulaire doit mettre en œuvre des mesures de cloisonnement appropriées entre le système d'information du service et ses autres systèmes d'information (bureautique, informatique de gestion, gestion technique du bâtiment, contrôle d'accès physique, etc.).

SAAS-CTLACC16 : Le candidat ou titulaire doit concevoir, développer, configurer et déployer le système d'information du service en assurant au moins un cloisonnement entre d'une part l'infrastructure technique et d'autre part les équipements nécessaires à l'administration des services et des ressources qu'elle héberge.

6.4. CRYPTOLOGIE

Mise en garde ; pour les exigences SAAS-CRYPTO3, SAAS-CRYPTO4 et SAAS-CRYPTO5, vous devez répondre uniquement aux protocoles que vous utilisez. Pour les restantes indiquer dans la colonne Observations « NON CONCERNE »

SAAS-CRYPTO1 : Le candidat ou titulaire doit définir et mettre en œuvre un mécanisme de chiffrement empêchant la récupération des données du commanditaire en cas de réallocation d'une ressource ou de récupération du support physique. Cet objectif pourra être atteint en utilisant un chiffrement applicatif dans le périmètre du candidat ou titulaire, avec au moins une clé par commanditaire.

SAAS-CRYPTO2 : Le candidat ou titulaire doit utiliser une méthode de chiffrement des données respectant les règles et recommandations de l'ANSSI concernant le choix et le dimensionnement des mécanismes cryptographiques, version en vigueur.

SAAS-CRYPTO3 : Si le protocole *Transport Layer Security* (TLS) est mis en œuvre, le candidat ou titulaire doit appliquer les recommandations de l'ANSSI relatives à TLS, note technique n° SDE-NT35/ANSSI/SDE/NP du 19 août 2016.

SAAS-CRYPTO4 : Si le protocole IPsec est mis en œuvre, le candidat ou titulaire doit appliquer les recommandations de l'ANSSI relatives à IPsec, note technique n° DAT-NT 003/ANSSI/SDE/NP du 3 août 2015.

SAAS-CRYPTO5 : Si le protocole SSH est mis en œuvre, le candidat ou titulaire doit appliquer les recommandations de l'ANSSI : relatives à un usage sécurisé d'(Open)SSH, note technique n° DATNT-007/ANSSI/SDE/NP du 17 août 2015.

SAAS-CRYPTO6 : Le candidat ou titulaire doit mettre en place un chiffrement des données sur les supports amovibles et les supports de sauvegarde amenés à quitter le périmètre de sécurité physique du système d'information du service, en fonction du besoin de sécurité des données (voir exigence SAAS-ACT1 et SAAS-ACT2.).

6.5. SECURITE DE L'EXPLOITATION

SAAS-SECEXPLOIT1 : Le candidat ou titulaire doit informer au plus tôt le commanditaire de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le commanditaire.

SAAS-SECEXPLOIT2 : Le candidat ou titulaire doit documenter et mettre en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants. Le périmètre d'application de cette exigence sur le système d'information du service doit nécessairement contenir

les postes utilisateurs sous la responsabilité du candidat ou titulaire et les flux entrants sur ce même système d'information.

SAAS-SECEXPLOIT3 : Le candidat ou titulaire doit documenter et mettre en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.

SAAS-SECEXPLOIT4 : Le candidat ou titulaire doit documenter et mettre en œuvre une politique de journalisation incluant au minimum les éléments suivants :

- la liste des sources de collecte ;
- la liste des événements à journaliser par source ;
- la fréquence de la collecte et base de temps utilisée ;
- la durée de rétention locale et centralisée ;
- les mesures de protection des journaux (dont chiffrement et duplication) ;
- la localisation des journaux.

SAAS-SECEXPLOIT5 : Le candidat ou titulaire doit générer et collecter les événements suivants : les activités des utilisateurs liées à la sécurité de l'information, la modification des droits d'accès dans le périmètre de sa responsabilité, les événements issus des mécanismes de lutte contre les codes malveillants, les exceptions, les défaillances et tout autre événement lié à la sécurité de l'information.

SAAS-SECEXPLOIT6 : Le candidat ou titulaire doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires.

SAAS-SECEXPLOIT7 : Le candidat ou titulaire doit fournir, sur demande d'un commanditaire, l'ensemble des événements le concernant.

SAAS-SECEXPLOIT8 : Le candidat ou titulaire doit protéger les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité.

SAAS-SECEXPLOIT9 : Le candidat ou titulaire doit mettre en place une sauvegarde des événements collectés suivant une politique adaptée.

SAAS-SECEXPLOIT10 : Le candidat ou titulaire doit exécuter les processus de journalisation et de collecte des événements avec des comptes disposant de privilèges nécessaires et suffisants. Il doit limiter l'accès aux événements journalisés conformément à la politique de contrôle d'accès.

6.6. INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION

SAAS-INCSSI : Le Titulaire doit assurer la traçabilité des incidents de sécurité des systèmes d'information et prévenir le RNSSI de l'EFS. Si un incident survient, cela implique un écart avec une ou plusieurs exigences de sécurité des systèmes d'information. Un rapport précis devra être produit et indiquer les actions à mettre œuvre pour remettre à niveau la ou les exigences et cela en commun accord entre le RSSI du Titulaire et la RNSSI de l'EFS.

6.7. LOCALISATION DES DONNEES

SAAS-LOC DATA1 : Le candidat ou titulaire doit documenter et communiquer au commanditaire la localisation du stockage et du traitement des données.

SAAS-LOC DATA2 : Le candidat ou titulaire doit stocker et traiter les données du commanditaire au sein la France ou l'Union Européenne.

SAAS-LOC DATA3 : Les opérations d'administration et de supervision du service doivent être réalisées depuis la France ou l'Union Européenne.

7. RELATIONS AVEC LES TIERS

RELSTIERS1 : Le candidat ou titulaire doit tenir à disposition du commanditaire la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de soustraitants au sens de l'article 28 du [RGPD] afin que le commanditaire puisse émettre des objections à cet égard.

RELSTIERS2 : Le candidat ou titulaire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le candidat ou titulaire doit inclure ces exigences dans les contrats conclus avec les tiers.

RELSTIERS3 : Le candidat ou titulaire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent document.

RELSTIERS4 : Le candidat ou titulaire doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

RELSTIERS5 : Le candidat ou titulaire doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences de ce recueil d'exigences.

RELSTIERS6 : Le candidat ou titulaire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgence vis-à-vis des tiers participant à la mise en œuvre du service.

8. FIN DU CONTRAT

FINCONTR1 : À la fin du contrat liant le candidat ou titulaire et le commanditaire, que le contrat soit arrivé à son terme ou pour toute autre cause, le candidat ou titulaire doit assurer un effacement sécurisé de l'intégralité des données du commanditaire. Cet effacement peut être réalisé suivant l'une des méthodes suivantes, et ce dans un délai précisé dans le contrat :

- effacement par réécriture complète de tout support ayant hébergé ces données ;
- effacement des clés utilisées pour le chiffrement des espaces de stockage du commanditaire ; - recyclage sécurisé, dans les conditions énoncées dans l'exigence FINCONTR 3.

FINCONTR2 : À la fin du contrat, le candidat ou titulaire doit supprimer les données techniques relatives au commanditaire (annuaire, certificats, configuration des accès, etc.)

FINCONTR3 : Le candidat ou titulaire doit documenter et mettre en œuvre des moyens permettant d'effacer de manière sécurisée par réécriture de motifs aléatoires tout support de données mis à disposition d'un commanditaire. Si l'espace de stockage est chiffré, l'effacement peut être réalisé par un effacement sécurisé de la clé de chiffrement.

FINCONTR4 : La suppression des données ne pourra être réalisée qu'une fois la réversibilité finalisée et un procès-verbal signé par le client.

9. PLAN DE CONTINUITE D'ACTIVITE

PCA1 : Un plan de continuité d'activité, formalisé et testé doit permettre de prévenir ou de subvenir à toute panne grave ou à tout sinistre impactant les obligations définies dans le Contrat.
Ce plan de continuité assure à minima la sauvegarde régulière des informations et applications.

10. PLAN D'ASSURANCE SECURITE (PAS)

PASSEC1 : Une fois la fin de la consultation et le choix d'un titulaire, ce dernier produira un plan d'assurance sécurité avec les exigences de sécurité indiquées dans ce document, en fonction de sa prestation.

Le PAS doit décrire les mesures de sécurité de l'EFS et mises en œuvre ainsi que leurs modalités d'application, sans que cette description ne puisse en aucun cas limiter l'obligation de résultat souscrite par le candidat ou titulaire de respecter le niveau minimal de sécurité.

PASSEC2 : Le PAS sera appliqué et tenu à jour par le candidat ou titulaire.

PASSEC3 : Un tableau de bord indiquant l'état de la conformité des exigences de sécurité doit être fourni par le titulaire à une fréquence définie en commun accord entre le RSSI du titulaire et la RNSSI de l'EFS. Si des écarts sont constatés, le titulaire devra indiquer un plan d'action afin que l'exigence soit couverte. Des réunions de suivi devront être planifiées pour démontrer la couverture de l'exigence.

11. AUDITS DE SECURITE

AUDSEC1 : L'EFS se réserve la possibilité de réaliser des audits de sécurité destinés à vérifier le respect par le candidat ou titulaire de son obligation de respecter le niveau de sécurité exigé par l'EFS et notamment de la bonne application du plan d'assurance sécurité. Le candidat ou titulaire sera prévenu de l'occurrence d'un audit au moins 5 jours ouvrés avant sa réalisation.

AUDSEC2 : Un plan d'actions doit être soumis par le candidat ou titulaire à l'EFS pour approbation du RNSSI au plus tard 15 jours après la livraison du rapport.

AUDSEC3 : Les écarts constatés avec le plan d'assurance sécurité et, plus généralement, tout nonrespect du niveau de sécurité de l'EFS devra être régularisés dans un délai convenu en commun accord entre les deux parties.

AUDSEC4 : l'EFS se réserve le droit d'accès à l'ensemble des documents relatifs à la sécurité du candidat ou titulaire dans le cadre de sa prestation.

AUDSEC5 : Les écarts importants constatés avec le plan d'assurance sécurité et, plus généralement, ou non-respect du niveau de sécurité demandé par l'EFS peuvent être une cause de rupture de contrat dans les conditions prévues dans le DCE.

AUDSEC6 : Afin de vérifier le respect des engagements définis dans le contrat, l'EFS peut procéder ou faire procéder à des audits et des contrôles des procédures mises en œuvre par le candidat ou titulaire.

AUDSEC7 : Les vulnérabilités identifiées lors de tests de sécurité devront être comblées par des mesures appropriées sur la base d'un plan d'actions validé par l'EFS (notamment le RNSSI) et le PAS sera mis à jour en conséquence.

ANNEXE 1 : MATRICE DE CONFORMITE

Comment remplit cette matrice

1. Cocher la case correspondante *CONFORME* ou *NON-CONFORME*.
2. Indiquer dans la colonne *OBSERVATIONS*, **la référence du document / ou du paragraphe traitant l'exigence dans la réponse au besoin.**
Nous faire parvenir obligatoirement l'ensemble de la documentation citée.
3. Si vous cochez une case *NON-CONFORME*, vous êtes dans l'obligation d'indiquer les raisons dans la colonne *OBSERVATIONS*.

DOMAINES	REFERENCE EXIGENCE	CONFORME	NON- CONFORME	OBSERVATIONS
SECURITE ORGANISATIONNELLE	SECORG1			
	SECORG2			
	SECORG3			
	SECORG4			
	SECORG5			
	SECORG6			
	SECORG7			
	SECORG8			
	SECORG9			
	SECINF-AUTOM1			
	SECINF-AUTOM2			
	SECINF-AUTOM3			
	SECINF-AUTOM4			
	SECINF-AUTOM5			
	SECINF-AUTOM6			
	SECINF-AUTOM7			
	SECDEV-GESTIDEN1			
	SECDEV-GESTIDEN2			
	SECDEV-AUTHENCENTRE			
	SECDEV-CHIFFREDATA1			
	SECDEV-CHIFFREDATA2			
	SECDEV-JOURNAUX			
	SECDEV-PROTECAPPLI1			
	SECDEV-PROTECAPPLI1			
	SECDEV-PROTECDATASEN			
	SECDEV-SECUAPPLI			

SECURITE INFORMATIQUE	SECDEV-SECURISE			
	SECDEV-VALIDDATA			
	SECDEV-MOINDRE PRIV			
	SECDEV-BIBLIOEXT			

	SECDEV-SECU SRVRS			
	SECDEV-REINCIDENTS			
	SECDEV-VERSIONNING –			
	SECDEV-REGLESNORMES			
	SECDEV-ANACODE			
	SECDEV MAJ DEPEND			
	SECDEV-TESTAUDITS			
	SECDEV-AUDITCONFO			
	SECDEV-CRYPTO			
	SECDEV-GESCLES			
	SECDEV-FORMSENS			
	SECDEV-ANALYSE			
	SECDEV-SVGD HSITE			
MAINTENANCE	MAINTEN1			
	MAINTEN2			
	MAINTEN3			
	MAINTEN4			
	MAINTEN5			
	MAINTEN6			
	MAINTEN7			
	MAINTEN8			
	MAINTEN9			
	MAINTEN10			
	MAINTEN11			
	MAINTEN12			
TELEMAINTENANCE	TELEMAIN1			
	TELEMAIN2			
	TELEMAIN3			
	TELEMAIN4			
	TELEMAIN5			
	TELEMAIN6			
	TELEMAIN7			
	TELEMAIN8			

	TELEMAIN9			
	TELEMAIN10			
	TELEMAIN11			
	TELEMAIN12			
	TELEMAIN13			
	TELEMAIN14			
	TELEMAIN15			
	TELEMAIN16			

	TELEMAIN17			
	TELEMAIN18			
	TELEMAIN19			
	TELEMAIN20			
	TELEMAIN21			
SAAS	SAAS-GEN1			
	SAAS-GEN2			
	SAAS-GEN3			
	SAAS-GESACT1			
	SAAS-GESACT2			
	SAAS-GESACT3			
	SAAS-CTLACC1			
	SAAS-CTLACC2			
	SAAS-CTLACC3			
	SAAS-CTLACC4			
	SAAS-CTLACC5			
	SAAS-CTLACC6			
	SAAS-CTLACC7			
	SAAS-CTLACC8			
	SAAS-CTLACC9			
	SAAS-CTLACC11			
	SAAS-CTLACC12			
	SAAS-CTLACC13			
	SAAS-CTLACC14			
	SAAS-CTLACC15			
	SAAS-CTLACC16			
	SAAS-CRYPTO1			
	SAAS-CRYPTO2			
	SAAS-CRYPTO3			

	SAAS-CRYPTO4			
	SAAS-CRYPTO5			
	SAAS-CRYPTO6			
	SAAS-SECEXPLOIT1			
	SAAS-SECEXPLOIT2			
	SAAS-SECEXPLOIT3			
	SAAS-SECEXPLOIT4			
	SAAS-SECEXPLOIT5			
	SAAS-SECEXPLOIT6			
	SAAS-SECEXPLOIT7			
	SAAS-SECEXPLOIT8			
	SAAS-SECEXPLOIT9			
	SAAS-SECEXPLOIT10			
	SAAS-INCSSI			
	SAAS-LOC DATA1			
	SAAS-LOC DATA2			
	SAAS-LOC DATA3			
RELATIONS AVEC LES TIERS	RELSTIERS1			
	RELSTIERS2			
	RELSTIERS3			
	RELSTIERS4			
	RELSTIERS5			
	RELSTIERS6			
FIN DU CONTRAT	FINCONTR1			
	FINCONTR2			
	FINCONTR3			
	FINCONTR4			
PLAN DE CONTINUITE D'ACTIVITE	PCA1			
PLAN D'ASSURANCE SECURITE	PASSEC1			
	PASSEC2			
	PASSEC3			
AUDITS DE SECURITE	AUDSEC1			
	AUDSEC2			
	AUDSEC3			
	AUDSEC4			
	AUDSEC5			
	AUDSEC6			
	AUDSEC7			

