

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

HISTORIQUE DES VERSIONS					
VERSION	DATE	OBSERVATIONS	REDACTEUR	VERIFICATEUR	APPROBATEUR
1.0	21/07/2021	Création du document	Maricela Pélegrin-Bomel RNSSI		
3.3	05/11/2025	Intégration des exigences de sécurité pour l'Intelligence Artificielle	Jules SARRAT RNSSI adjoint		

SOMMAIRE

1. INTRODUCTION	3
2. SECURITE ORGANISATIONNELLE	4
3. SECURITE INFORMATIQUE	4
3.1. GENERALITES	4
3.2. SPECIFICITES POUR LES AUTOMATES	6
4. TELEMANTENANCE AUTOMATES	7
4.1. TELEMANTENANCE	7
4.2. MAINTENANCE PREDICTIVE	8
5. FOURNITURE DE SERVICE SAAS (SOFTWARE AS A SERVICE)	8
5.1. GENERALITES	8
5.2. GESTION DES ACTIFS	8
5.3. CONTROLE D'ACCES ET GESTION DES IDENTITES	8
5.3.1. Contrôle d'accès	8
5.4. CRYPTOLOGIE	10
5.5. SECURITE DE L'EXPLOITATION	10
5.6. INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION	11
5.7. LOCALISATION DES DONNEES	11
6. RELATIONS AVEC LES TIERS	11
7. FIN DU CONTRAT	12
8. PLAN DE CONTINUITE D'ACTIVITE	12
9. PLAN D'ASSURANCE SECURITE (PAS)	12
10. AUDITS DE SECURITE	12
ANNEXE 1 : MATRICE DE CONFORMITE	14

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
IA	Intelligence Artificielle
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 Ce service concerne la mise à disposition par le titulaire d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le 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

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.

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 informatique, les exigences SaaS, la télémaintenance, la relations avec les tiers et le plan de continuité d'activité y sont présentés.

Le titulaire est invité à prendre connaissance des mesures de sécurité listées, indiquer son niveau de conformité pour chacune d'entre elles et à y apporter une réponse complémentaire sous forme d'un Plan d'Assurance Sécurité.

Le titulaire doit garder à l'esprit qu'une non-conformité n'est pas un blocage. 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.
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 titulaire ayant le visa SecNumCloud et/ou Cloud de Confiance de l'ANSSI. Le 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 pour le Titulaire du service

En réponse à nos exigences il est impératif de :

- Les intégrer dans la conception et/ou réalisation des produits ou prestations ;
- Compléter la matrice de conformité en annexe pour préciser si le titulaire est conforme ou non aux exigences du présent document ;
- Fournir un Plan d'Assurance Sécurité basé sur les exigences listées ci-après.

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

3. SECURITE INFORMATIQUE

3.1. GENERALITES

SECINF1 : Le système d'information est protégé contre les intrusions physiques et informatiques en provenance de l'extérieur et contre les actes de malveillance interne.

SECINF2 : Les accès aux informations relatives à l'EFS, aux donneurs et aux receveurs doivent être techniquement limités au strict nécessaire à l'accomplissement des prestations (contrôle d'accès aux applications et machines, séparation physique...).

SECINF3 : L'accès aux services par les utilisateurs doit faire l'objet d'une d'authentification par mot de passe renforcer devant respecter la politique suivante :

- Longueur minimale de 12 caractères, mélangeant lettres majuscules et minuscules, chiffres et caractères spéciaux (exemple : #, [, !, ^, etc.) ;
- Durée de validité du mot de passe fixée à 120 jours ;
- Non-réutilisation des cinq derniers mots de passe ;
- Nombre de tentatives pour la saisie du mot de passe limité à 3 puis blocage du compte.

Dans le cadre des administrateurs ceux derniers doivent suivre les règles suivantes :

- Longueur minimale de 16 caractères, mélangeant lettres majuscules et minuscules, chiffres et caractères spéciaux (exemple : #, [, !, ^, etc.) ;
- Durée de validité du mot de passe fixée à 120 jours ;
- Non-réutilisation des cinq derniers mots de passe ;
- Nombre de tentatives pour la saisie du mot de passe limité à 3, puis blocage du compte

SECINF4 : Des outils de chiffrement (« *cryptage* ») doivent être mis en œuvre.

Les moyens de chiffrements utilisés doivent être autorisés par la loi française. Ils devront utiliser des moyens cryptographiques forts. A ce titre, l'usage d'une clé de longueur de 256 bits pour un mécanisme

de chiffrement approuvé par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est obligatoire. A date, l'*Advanced Encryption Standard* (AES) semble être un minimum.

SECINF5 : Les clés de déchiffrement ne sont communiquées qu'aux personnes ayant signé un accord de confidentialité. Ces personnes s'engagent dans cet accord à ne pas divulguer ces clés.

SECINF6 : Les fichiers de l'EFS ne doivent pas être dupliqués ni transmis à un tiers sans l'accord de de l'EFS.

SECINF7 : Toute transmission de fichiers sur un support physique (CDROM, clé USB...), par courrier externe ou par porteur donnera lieu à un accusé de réception. Il devra respecter les règles de protection des informations indiquées par le Prescripteur.

SECINF8 : Chaque personne qui accède à des ressources informatiques ou réseau dispose d'un compte individuel qui est un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au long de la vie du compte.

SECINF9 : Les mots de passe des comptes utilisés par les applications et les traitements automatisés doivent être changés au moins tous les 6 mois. Ils ne doivent être accessibles et modifiables que par l'exploitant de ce traitement. La politique pour ces mots de passe doit être la suivante :

- Les mots de passe doivent être composés d'au minimum de 16 caractères comprenant des majuscules, des minuscules et des chiffres, avec un caractère spécial obligatoire ;
- Nombre de tentatives d'authentification : 5 maximum ;
- Période de blocage après le nombre de tentatives ci-dessous : 5 minutes (ceci pour réduire la probabilité d'authentification frauduleuse par force brute) ;
- Si le mot de passe est à envoyer, il doit se faire de manière chiffrée ;
- Effectuer un contrôle de la robustesse et de la politique de constitution du mot de passe dès sa création et de son renouvellement.
- Le mot de passe doit être obligatoirement conservé dans un coffre-fort des mots de passe.
- Si constat ou suspicion de compromission du mot de passe, obligation de son changement dès que possible et cela avant 24h00.
- Interdire l'utilisation des 5 derniers mots de passe.
- Durée d'utilisation du mot de passe 180 jours.

SECINF10 : La résistance des mots de passe est suivie et contrôlée de façon à ce que ceux-ci ne soient pas devinables, c'est-à-dire qu'ils ne sont pas une dérivation simple du login de l'utilisateur, de son nom, de son prénom, d'une date, d'un nom commun, d'un prénom ou d'un nom propre en langue française, anglaise ou de celle du pays dans lequel sont implantés les locaux du titulaire.

SECINF11 : L'accès aux secrets qui permettent l'authentification des utilisateurs (bases de mots de passe en clair, hachées ou chiffrées, ...) est interdit.

SECINF12 : Les moyens d'authentification incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

SECINF13 : Les journaux des événements de sécurité doivent être conservés sur 12 mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

SECINF14 : Les traces doivent pouvoir être imputables à un individu. Elles sont horodatées selon une référence horaire commune à l'ensemble de l'entreprise.

SECINF15 : Les informations minimales qui sont collectées et stockées sont :

- Connexion et déconnexion aux équipements et applications ;
- Consultations d'informations relatives à la vie privée de nos donneurs, receveurs et de nos collaborateurs ;
- Informations d'usage de l'Internet (accès aux sites Web) ;
- Accès en lecture et en écriture à des fichiers et dossiers classifiés « *Confidentiel* »

SECINF16 : Les sauvegardes informatiques sont faites régulièrement et traitées de manière à garantir leur disponibilité, confidentialité et leur intégrité.

- Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.
- Les sauvegardes de données devront être effectuées sur un site différent et distant.

SECINF17 : L'architecture mise en œuvre pour la plate-forme ou SI de l'EFS hébergée chez un titulaire permettra d'assurer la disponibilité du service.

SECINF18 : Le titulaire doit documenter les procédures d'exploitation, les tenir à jour et les rendre accessibles au personnel concerné.

SECINF19 : Le système d'information hébergé doit être protégé contre les attaques virales et les intrusions informatiques.

SECINF20 : Le titulaire hébergeur devra assurer le suivi des vulnérabilités des équipements de sécurité et appliquer les correctifs aux systèmes de sécurité sur les systèmes d'exploitation des serveurs ou applications.

SECINF21 : 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.

SECINF27 : Le Titulaire doit maintenir à jour ses équipements réseau, ses systèmes d'exploitation et ses applications avec les derniers correctifs de sécurité.

SECINF28 : Le Titulaire doit mettre en place des outils de contrôle du trafic (entrant et sortant) de données avec le SI de l'EFS, ainsi que des outils de surveillance réseau pour détecter et répondre aux activités suspectes ou aux intrusions afin de bloquer les menaces potentielles.

SECINF29 : Le Titulaire doit effectuer des analyses régulières des vulnérabilités pour identifier et corriger les failles de sécurité.

SECINF30 : Le Titulaire doit utiliser des protocoles de routage sécurisés pour empêcher les attaques d'usurpation ou de détournement.

3.2. 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 anti-virus à jour au niveau de ses bases de signatures ou station-blanche. 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 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 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 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 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)

4. TELEMAINTENANCE AUTOMATES

4.1. TELEMAINTENANCE

TELEMAIN1 : Les accès en télémaintenance sont autorisés uniquement via les systèmes (réseau, solution, prise en main à distance, etc...) validés par l'EFS.

TELEMAIN2 : La connexion de télémaintenance du titulaire doit se faire via un service sécurisée mise à disposition par l'EFS conformément à sa politique de sécurité.

TELEMAIN3 : 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.

TELEMAIN4 : Tout accès fera l'objet d'une demande d'approbation par le métier au moment de la connexion par le tiers.

TELEMAIN5 : Tout accès sera tracé (horodatage de la connexion et des actions réalisées par le tiers).

TELEMAIN6 : Le formulaire d'habilitation transmis par l'EFS devra être dûment complété par le tiers avant la création d'un accès en télémaintenance.

TELEMAIN7 : Tout compte d'accès doit être nominatif et fera l'objet d'une fiche d'habilitation individuelle.

TELEMAIN8 : Le tiers s'engage à informer sans délai l'EFS en cas mouvement de personnel.

TELEMAIN9 : 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.

TELEMAIN10 : Le tiers devra procéder à une revue d'habilitation annuelle des comptes actifs.

TELEMAIN11 : L'EFS se réserve le droit de couper, sans préavis, son accès internet ou à son réseau en cas de force majeure.

TELEMAIN12 : 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.

TELEMAIN13 : L'accès distant ne sera permis que depuis des plages d'adresses IP déclarées par le télémainteneur.

4.2. MAINTENANCE PREDICTIVE

TELEMAIN14 : Toute demande de mise en place de maintenance prédictive devra faire l'objet d'une demande préalable détaillant, outre la nature des données, la volumétrie et la fréquence des échanges

TELEMAIN15 : L'EFS se réserve le droit d'auditer le trafic entre l'automate et le serveur distant

TELEMAIN16 : 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

5. FOURNITURE DE SERVICE SAAS² (SOFTWARE AS A SERVICE)

5.1. GENERALITES

SAAS-GEN1 : 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

5.2. 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.

5.3. CONTROLE D'ACCES ET GESTION DES IDENTITES

5.3.1. CONTROLE D'ACCES

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

² Ce service concerne la mise à disposition par le titulaire d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le 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-CTLACC2 : Le 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 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 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.

SAAS-CTLACC5 ; Le 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 titulaire ou du commanditaire ainsi que les droits d'accès qui leurs ont été attribués.

SAAS-CTLACC6 : Le titulaire doit être en mesure de fournir, pour un utilisateur donné, qu'ils soient sous la responsabilité du 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 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 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 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 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 titulaire doit mettre en place un système d'authentification à double facteur pour l'accès : aux interfaces d'administration utilisées par le 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 titulaire doit mettre en œuvre des mesures de cloisonnement appropriées entre ses commanditaires.

SAAS-CTLACC15 : Le 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 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.

5.4. 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 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 titulaire, avec au moins une clé par commanditaire.

SAAS-CRYPTO2 : Le 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 titulaire doit appliquer les recommandations de l'ANSSI relatives à TLS, note technique n° SDE-NT-35/ANSSI/SDE/NP du 19 août 2016.

SAAS-CRYPTO4 : Si le protocole IPsec est mis en œuvre, le 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 titulaire doit appliquer les recommandations de l'ANSSI : relatives à un usage sécurisé d'(Open)SSH, note technique n° DAT-NT-007/ANSSI/SDE/NP du 17 août 2015.

SAAS-CRYPTO6 : Le 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.).

5.5. SECURITE DE L'EXPLOITATION

SAAS-SECEXPLOIT1 : Le 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 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 titulaire et les flux entrants sur ce même système d'information.

SAAS-SECEXPLOIT3 : Le 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 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 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 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 titulaire doit fournir, sur demande d'un commanditaire, l'ensemble des événements le concernant.

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

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

SAAS-SECEXPLOIT10 : Le 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.

5.6. 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.

5.7. LOCALISATION DES DONNEES

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

SAAS-LOC DATA2 : Le 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.

6. RELATIONS AVEC LES TIERS

RELSTIERS1 : Le 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 sous-traitants au sens de l'article 28 du RGPD afin que le commanditaire puisse émettre des objections à cet égard.

RELSTIERS2 : Le 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 titulaire doit inclure ces exigences dans les contrats conclus avec les tiers.

RELSTIERS3 : Le 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 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 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 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-divulgaration vis-à-vis des tiers participant à la mise en œuvre du service.

7. FIN DU CONTRAT

FINCONTR1 : À la fin du contrat liant le titulaire et le commanditaire, que le contrat soit arrivé à son terme ou pour toute autre cause, le 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 titulaire doit supprimer les données techniques relatives au commanditaire (annuaire, certificats, configuration des accès, etc.)

FINCONTR3 : Le 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.

8. 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.

9. PLAN D'ASSURANCE SECURITE (PAS)

PASSEC1 : Un plan d'assurance sécurité doit être produit sur la base des présentes 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 titulaire de respecter le niveau minimal de sécurité.

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

10. AUDITS DE SECURITE

AUDSEC1 : L'EFS se réserve la possibilité de réaliser des audits de sécurité destinés à vérifier le respect par le 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 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 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 non-respect 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 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.

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 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.