

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

SOMMAIRE

1. INTRODUCTION	3
2. SECURITE ORGANISATIONNELLE.....	5
3. SECURITE PHYSIQUE DES LOCAUX	6
3.1. EXPOSITION AUX RISQUES	6
3.2. REFERENTIELS APPLICABLES.....	6
3.3. PROTECTION CONTRE L'INTRUSION	6
3.4. TELESURVEILLANCE.....	6
3.5. SECURITE INCENDIE.....	6
3.6. PROTECTION CONTRE LES DEGATS DES EAUX	7
3.7. MAINTIEN EN CONDITIONS OPERATIONNELLES DES EQUIPEMENTS DE SECURITE	7
4. SECURITE INFORMATIQUE	8
5. FOURNITURE DE SERVICE SAAS (SOFTWARE AS A SERVICE).....	11
5.1. GENERALITES	11
5.2. GESTION DES ACTIFS	12
5.3. CONTROLE D'ACCES ET GESTION DES IDENTITES	12
5.3.1. Contrôle d'accès	12
5.4. CRYPTOLOGIE.....	13
5.5. SECURITE DE L'EXPLOITATION.....	14
5.6. RELATIONS AVEC LES TIERS	14
5.7. INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION	15
5.8. LOCALISATION DES DONNEES	15
5.9. FIN DU CONTRAT.....	15
6. RELATIONS AVEC LES TIERS	17
7. FIN DU CONTRAT.....	17
8. PLAN DE CONTINUITE D'ACTIVITE	18
9. PLAN D'ASSURANCE SECURITE (PAS)	19
10. AUDITS DE SECURITE.....	19

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 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

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 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 candidat 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 Physique des locaux	Réponse obligatoire dans le cas où la prestation se réalisera en dehors des locaux de l'EFS
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.
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 lors de la soumission de l'offre.

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 PHYSIQUE DES LOCAUX

Mise en garde : si vous faites appel à un prestataire d'hébergement pour votre solution, les réponses à ces exigences doivent être les siennes. Vous devez obtenir une réponse de sa part

A contrario, si vous hébergez votre solution dans votre propre Datacenter, c'est à vous qu'incombe la réponse à ces exigences.

3.1. EXPOSITION AUX RISQUES

SECPHY-ER1 : L'implantation géographique des locaux ne doit pas être exposée à des risques naturels ni à des risques sociaux ou industriels. Toutefois, si les locaux sont implantés dans une zone présentant des risques, le candidat ou titulaire devra décliner la manière dont ces risques sont pris en compte pour assurer la continuité de service.

3.2. REFERENTIELS APPLICABLES

SECPHY-RA1 : En complément des dispositions législatives et réglementaires en vigueur, toutes les installations concourant à la sécurité physique des locaux doivent respecter les règles françaises APSAD (Assemblée Plénière des Sociétés d'Assurance Dommage).

3.3. PROTECTION CONTRE L'INTRUSION

SECPHY-PL1 : Les locaux du candidat ou titulaire doivent être équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements doivent être opérationnels 24h/24h et 7j/7j.

Les moyens de protection doivent être adaptés aux moyens de détection et de réaction.

SECPHY-PL2 : Les accès physiques doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du candidat ou titulaire.

SECPHY-PL3 : Le système de vidéosurveillance, s'il existe, doit être configuré de manière à permettre l'exploitation des enregistrements quelles que soient les conditions d'éclairage. Les images doivent être d'une qualité suffisante pour permettre de reconnaître les personnes quelles que soient les conditions.

SECPHY-PL4 : Le candidat ou titulaire doit assurer la traçabilité des incidents de sécurité.

3.4. TELESURVEILLANCE

SECPHY-TSV1 : Si la surveillance des locaux est confiée à une société de télésurveillance, ses délais d'intervention sur site ne doivent pas dépasser 20 minutes. Les alarmes qui lui sont transmises doivent être différenciées en fonction des événements, au minimum :

- Incendie ;
- Intrusion ;
- Dégâts des eaux si détection de liquides ;
- Autres alarmes critiques de gestion technique centralisée du bâtiment.

3.5. SECURITE INCENDIE

SECPHY-SI1 : Les installations de protection incendie doivent respecter les dispositions législatives et réglementaires et être conformes aux règles APSAD².

SECPHY-SI2 : Les locaux doivent être protégés contre les effets directs et indirects de la foudre.

² Assemblée Plénière de Sociétés d'Assurances Dommages

SECPHY-SI3 : Les travaux sur points chauds (soudure, meulage, ...) doivent donner lieu à la rédaction d'un permis de feu et faire l'objet d'une vigilance particulière.

SECPHY-SI4 : L'accès aux extincteurs doit être dégagé en permanence. Une signalétique appropriée doit permettre de les localiser.

SECPHY-SI5 : Le candidat ou titulaire veille à éliminer quotidiennement tout potentiel calorifique inutile de ses locaux (emballages, palettes, déchets de toute nature). Les conteneurs de déchets (bennes) et les stocks de palettes doivent être disposés à une distance minimale de 10 mètres des locaux.

3.6. PROTECTION CONTRE LES DEGATS DES EAUX

SECPHY-PGE1 : Le cheminement des canalisations doit se faire hors des locaux sensibles.

SECPHY-PGE2 : Les zones à caractère stratégique doivent être équipées d'un système de détection

SECPHY-PGE3 : Les canalisations apparentes doivent être protégées contre les chocs.

SECPHY-PGE4 : Les installations de plomberie doivent faire l'objet d'un contrat de maintenance.

SECPHY-PGE5 : Les gouttières, avaloirs, exutoires d'eau pluviale, etc. doivent être curés au minimum une fois par an, de préférence en fin d'automne pour éliminer les feuilles mortes.

3.7. MAINTIEN EN CONDITIONS OPERATIONNELLES DES EQUIPEMENTS DE SECURITE

SECPHY-MCO1 : L'infrastructure technique des bâtiments (distribution d'énergie et de fluides, climatisation des locaux) doit être redondante.

SECPHY-MCO2 : Les équipements de sécurité (incendie, intrusion, surveillance vidéo, ...) doivent disposer d'une alimentation électrique de secours d'une autonomie minimale de 4 heures.

SECPHY-MCO3 : L'ensemble des équipements qui concourent à la sécurité et à la continuité des opérations doit faire l'objet d'un contrat de maintenance préventive et doit satisfaire aux visites périodiques de contrôle telles que prévues dans les règles APSAD et dans la réglementation française.

SECPHY-MCO4 : En particulier, les installations électriques doivent faire l'objet d'un contrôle annuel renforcé par thermographie infrarouge.

SECPHY-MCO5 : Le candidat ou titulaire tient à jour un registre de sécurité regroupant les certificats de conformité, les procès-verbaux de visites réglementaires et le compte rendu des actions correctives réalisées, sur lequel doivent figurer l'identité des personnes les ayant réalisées et à quelle date.

4. SECURITE INFORMATIQUE

4.1. GENERALITES

Le candidat ou titulaire mettra en œuvre les mesures de sécurité suivantes :

SECINF1 : Le système d'information bénéficie d'une alimentation électrique de secours d'une autonomie minimale de 4 heures.

SECINF2 : Le système d'information est protégé contre les intrusions physiques et informatiques en provenance de l'extérieur et contre les actes de malveillance interne.

SECINF3 : 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, ...).

SECINF4 : L'accès aux serveurs 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

SECINF5 : Les modalités d'échanges d'informations permettent d'en assurer la confidentialité et l'intégrité. Elles doivent permettre d'authentifier les entités en communication.

Le candidat ou titulaire s'engage à suivre les procédures suivantes :

- Toute donnée « *Confidentielle* » échangée doit être chiffrée, quel que soit le réseau utilisé ;
- Tout chiffrement sera réalisé avec les normes et outils homologués par l'EFS. Les outils de chiffrement seront choisis dans le catalogue des solutions homologuées par l'ANSSI. Les principes pour la classification des données (« *Confidentielle* », à « *Non Protégé* », etc...) sont énoncés par le Prescripteur.

SECINF6 : 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.

SECINF7 : 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.

SECINF8 : Les fichiers de l'EFS ne doivent pas être dupliqués ni transmis à un tiers sans l'accord de de l'EFS.

SECINF9 : Les fichiers de l'EFS devront être effacés physiquement des supports d'information à l'issue de la prestation, y compris des supports de sauvegarde. Un procès-verbal de destruction doit être présenté.

SECINF10 : 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.

SECINF11 : Chaque personne qui accède à des ressources informatiques ou réseau dispose d'un compte individuel qui peut être :

- Soit un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte ;
- Soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

SECINF12 : Des comptes individualisés peuvent être utilisés à condition que des moyens non contournables soient mis en place pour imputer sans ambiguïté les actions faites avec chaque compte à leur auteur.

SECINF13 : En cas de nécessité (requête des autorités, cas de malveillance, ...), le candidat ou titulaire doit être capable de révéler l'identité réelle de la personne qui utilisait un compte individualisé à un instant donné.

SECINF14 : Les mots de passe des utilisateurs doivent être changés au moins tous les 3 mois.

SECINF15 : 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.

SECINF16 : Les mots de passe des comptes utilisés par les applications doivent être constitués d'au moins 16 caractères alphanumériques qui combinent au moins des lettres majuscules et minuscules ainsi que des chiffres ou des caractères spéciaux.

SECINF17 : 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 candidat ou titulaire.

SECINF18 : L'accès aux secrets qui permettent l'authentification des utilisateurs (bases de mots de passe en clair, hachées ou chiffrées, ...) ne doit être donné qu'aux administrateurs de ces données, leurs accès doivent être tracés dans un référentiel. Les raisons de l'accès à ces données doivent être régulièrement analysées.

SECINF19 : Les moyens d'authentification incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

SECINF20 : 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.

SECINF21 : Les traces doivent pouvoir être imputables à un individu. Elles sont horodatées selon une référence horaire commune à l'ensemble de l'entreprise.

SECINF22 : 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* »

SECINF23 : 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.

SECINF24 : Dans le cadre spécifique de la sécurisation du réseau d'un candidat ou titulaire hébergeant tout ou partie de nos systèmes d'information, celui-ci s'engage à :

- Décrire les mesures de protection des données mis en place pour la gestion du réseau, ainsi que le processus d'administration du réseau ;
- Appliquer sur demande de l'EFS des mesures complémentaires pour protéger les équipements hébergés.

SECINF25 : L'architecture mise en œuvre pour la plate-forme ou SI de l'EFS hébergée chez un candidat ou titulaire permettra d'assurer la disponibilité du service.

SECINF26 : Le candidat ou titulaire doit documenter les procédures d'exploitation, les tenir à jour et les rendre accessibles au personnel concerné.

SECINF27 : Le système d'information hébergé doit être protégé contre les attaques virales et les intrusions informatiques.

SECINF28 : Le candidat ou 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.

SECINF29 : L'hébergement des données sur le territoire national ou européen est obligatoire³. En outre, l'hébergement de certaines données doit répondre aux exigences légales et réglementaires (données à caractère personnel, données de santé, ...).

SECINF30 : Le candidat ou titulaire doit s'engager contractuellement sur les mesures de sécurité qu'il met en œuvre pour la protection de la disponibilité, intégrité, confidentialité et traçabilité des données. Afin d'assurer leur confidentialité et disponibilité, les données sensibles ou indiquées comme « *Confidentielles* » par l'EFS, elles doivent être stockées de manière chiffrée et répliquées à intervalles réguliers dans la journée. Afin de répondre aux exigences du Référentiel Général de Sécurité (RGS), la solution de chiffrement doit faire partie du catalogue de solutions homologuées par l'ANSSI.

SECINF31 : L'accès par l'EFS à des données hébergées hors du réseau EFS doit se faire via un protocole sécurisé. L'hébergeur doit s'engager à mettre en place des protocoles de transmission permettant de garantir l'intégrité et la confidentialité des données transmises (utilisation des protocoles HTTPS, TLS etc.). Le chiffrement doit être garanti 256 bits minimum sur les navigateurs compatibles. Le suivi des recommandations de l'ANSSI doit être respecté.

SECINF32 : Afin de prévenir et d'analyser les incidents de sécurité des systèmes d'information et dans le but de satisfaire aux exigences de preuve et contrôle, une journalisation des accès aux données ou applications hébergées doit être mis en place par le candidat ou titulaire. Les conditions de journalisation (nature des informations, durée de conservation, modalités d'exploitation, etc.) doivent être fixées conjointement par les deux parties.

³ Circulaire n° 6404/SG du 31 mai 2023 sur l'actualisation de la doctrine d'utilisation de l'informatique en nuage par l'Etat (Cloud au centre) / Règle [R9]

Les moyens de surveillance et d'enregistrement doivent être signalés dans le contrat aux différentes parties, ainsi qu'aux autorités compétentes (CNIL) en cas d'enregistrement de données à caractères personnel.

SECINF33 : En cas d'expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le candidat ou titulaire s'engage :

- A éviter toute interruption et baisse de qualité des services ;
- A assurer les opérations qui permettront à l'EFS d'avoir toute la maîtrise nécessaire afin de reprendre ou de faire reprendre par un tiers les services dans les meilleures conditions (transfert de compétence, documents explicatifs, etc.).

SECINF34 : Lorsqu'il est mis fin à l'hébergement, le candidat ou titulaire doit restituer l'ensemble des données qui lui ont été confiées, sans en garder de copie. Un procès-verbal de suppression des données doit être fourni.

SECINF35 : 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.

SECINF36 : Le Titulaire doit maintenir à jour ses équipements réseau, ses systèmes d'exploitation et ses applications avec les derniers correctifs de sécurité.

SECINF37 : 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.

SECINF38 : Le Titulaire doit effectuer des analyses régulières des vulnérabilités pour identifier et corriger les failles de sécurité.

SECINF39 : Le Titulaire doit utiliser des réseaux privés virtuels (VPN) pour se connecter au réseau de L'EFS afin de sécuriser les connexions à distance et garantir la confidentialité des données.

SECINF40 : Le Titulaire doit utiliser des protocoles de routage sécurisés pour empêcher les attaques d'usurpation ou de détournement.

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

5.1. 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

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

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 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.

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.

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 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-NT-35/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° DAT-NT-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.).

5.5. 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.

5.6. RELATIONS AVEC LES TIERS

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

SAAS-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.

SAAS-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.

SAAS-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.

SAAS-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.

SAAS-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.

5.7. 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.

5.8. 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.

5.9. FIN DU CONTRAT

SAAS-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 décrit au chapitre 5.3 CRYPTOLOGIE ;
- recyclage sécurisé, dans les conditions énoncées dans l'exigence SAAS-FINCONTR 3.

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

SAAS-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.

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

6. 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 sous-traitants 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.

7. 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.

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 : 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.

10. 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 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 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.