

|  |
| --- |
| Exigences de Sécurité des Systèmes d’Information  Fourniture d’automates de séparation des produits sanguins labiles |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **HISTORIQUE DES VERSIONS** | | | | | |
| **VERSION** | **DATE** | **OBSERVATIONS** | **REDACTEUR** | **VERIFICATEUR** | **APPROBATEUR** |
| **1.0** | 20/01/2023 | Ajout d’information sur les non conformités | Maricela PELEGRIN-BOMEL  RNSSI |  |  |
| **1.1** | 9/11/2023 | Modification des règles des mots de passe  Changement des exigences :   * **SECINF22**:   Les mots de passe des comptes utilisés par les applications doivent être constitués d’au moins 16 caractères alphanuméri-ques | Maricela PELEGRIN-BOMEL  RNSSI |  |  |
| **2.0** | 1/02/2024 | Ajout de la sécurité physique | Maricela PELEGRIN-BOMEL  RNSSI |  |  |

**SOMMAIRE**

**\_\_\_\_\_\_\_\_\_\_**

1. INTRODUCTION 4

2. sécurité organisationnelle 5

3. Sécurité informatique 5

3.1. Généralités 5

4. TELEMAINTENANCE 10

4.1. Généralités 10

4.2. Maintenance sur site 11

4.3. Télémaintenance 11

4.4. maintenance PREDICTIVE 11

5. RELATIONS AVEC LES TIERS 12

6. FIN DU CONTRAT 12

7. Plan de Continuité d’activité 12

8. PLAN d’ASSURANCE sécurité (PAS) 13

9. Audits de sécurité 13

ANNEXE 1 : MATRICE DE CONFORMITE 14

**GLOSSAIRE :**

|  |  |
| --- | --- |
| **AES** | *Advanced Encryption Standard* |
| **ANSSI** | Agence Nationale de Sécurité des Systèmes d’Information |
| **APSAD** | Assemblée Plénière des Sociétés d’Assurance Dommage |
| **CCTP** | Cahier des clauses techniques particulières |
| **DCE** | Dossier de Consultation des Entreprises |
| **DCP** | Données à caractère personnel |
| **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 |
| **RNSSI** | Responsable National de la Sécurité des Systèmes d’Information |
| **RPA** | Représentant des pouvoirs adjudicateurs |
| **SI** | Systèmes d’Information |
| **SSI** | Sécurité des Systèmes d’Information |

# 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 imposées par les obligations légales de son activité.

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, la télémaintenance et le plan de continuité d’activité et le plan d’assurance sécurité y sont présentés.

Les candidats sont invités à prendre connaissance des mesures de sécurité indiquées et à y apporter une réponse dans le cadre 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 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 atteindre la conformité.

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.  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** | Réponse obligatoire pour toute action visant à maintenir et **contrôler à distance du matériel et/ou un système d’information** en difficulté. Ceci par le biais du réseau local ou Internet, afin de réaliser des opérations sur le système et/ou d’émettre un diagnostic devant permettre la résolution des problèmes d’équipement défectueux ainsi que sur le système 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.

# sécurité organisationnelle

**SECORG1** : Le candidat 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 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.

# Sécurité informatique

## Généralités

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

**SECINF1** :Seuls les progiciels nécessaires au fonctionnement des automates de séparation des produits sanguins labiles système sont installés.

* le candidat communique la liste exhaustive des services systèmes strictement nécessaires au fonctionnement attendu des automates ;
* tout service système installé sur un équipement induit un risque supplémentaire (vulnérabilités affectant le service exploitable) ;
* les services non nécessaires sont désactivés par le candidat lors de l’installation pour réduire tout usage malveillant. En désactivant les services annexes, on réduit la surface d’attaque.

**SECINF2** :Afin d’assurer la protection contre les codes malveillants : le système est équipé du dispositif de protection contre les codes malveillants (antivirus). Ce dispositif se met à jour quotidiennement à partir d’un serveur afin de bénéficier des dernières signatures et versions. Le logiciel antivirus installé sera l’antivirus EFS, en cas de besoin, le candidat informera l’EFS sur la liste des exclusions à effectuer pour l’analyse.

**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** : 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.

**SECINF5** : 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 candidat 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. Cette procédure est partie intégrante des procédures de maintenance sur site.

**SECINF6** : 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 candidat 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.

**SECINF7** : Les accès à distance pour la télémaintenance doivent être réalisés uniquement via la solution homologuée par l’établissement (MENTOR ou 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.

**SECINF8** : Le candidat 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 dans le présent Cahier des clauses techniques particulières. Il le fait conformément aux règles décrites dans la « Charte d’utilisation du système d’information de l’EFS » fournie en annexe 1 et en respectant les exigences de sécurité relatives à la (télé)maintenance sur les automates de l’EFS indiquées dans ces exigences.

**SECINF9** : Le candidat 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 candidat, 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 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 candidat s’engage à fournir un système d’exploitation dont le support est toujours assuré par l’éditeur.

**SECINF10** : 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) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**SECINF11** :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, ...).

**SECINF12** :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 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.

**SECINF13** :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.

**SECINF14** :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.

**SECINF15** :Les fichiers de l’EFS ne doivent pas être dupliqués ni transmis à un tiers sans l’accord de l’EFS.

**SECINF16** :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.

**SECINF17** :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.

**SECINF18** :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.

**SECINF19** :En cas de nécessité (requête des autorités, cas de malveillance, …), le candidat

doit être capable de révéler l’identité réelle de la personne qui utilisait un compte individualisé à un instant donné.

**SECINF20** : L’objet d’une d’authentification par mot de passe doit 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 pour les utilisateurs ;
* non-réutilisation des cinq derniers mots de passe ;
* nombre de tentatives pour la saisie du mot de passe limité à 3.

**SECINF21**: 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.**

**SECINF22**: 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.

**SECINF23**: 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’il 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.

**SECINF24**: 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.

**SECINF25**: Les moyens d’authentification incluent une protection contre les attaques en essai et erreur sur les secrets d’authentification.

**SECINF26**: 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.

**SECINF27**: Les traces doivent pouvoir être imputables à un individu. Elles sont horodatées selon une référence horaire commune à l’ensemble de l’entreprise.

**SECINF28** : 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.

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.

**SECINF29**: Le candidat doit documenter les procédures d’exploitation, les tenir à jour et les rendre accessibles au personnel concerné en langue française.

**SECINF30** : Le candidat 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

**SECINF31** : En cas d’expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le candidat s’engage :

* à éviter toute interruption et baisse de qualité des services ;
* à 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.).

**SECINF32** :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 sinistre que les données sauvegardées.

**SECINF33**: Le candidat doit documenter les procédures d’exploitation, les tenir à jour et les rendre accessibles au personnel concerné.

**SECINF34**: Le système d’information doit être protégé contre les attaques virales et les intrusions informatiques.

**SECINF35** : Le candidat 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.

**SECINF37**: L’hébergement des données sur le territoire national ou européen est obligatoire[[1]](#footnote-1). En outre, l’hébergement de certaines données doit répondre aux exigences légales et réglementaires (données à caractère personnel, données de santé, …).

**SECINF38** : Le candidat 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 le Prescripteur, 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.

**SECINF39** : 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/SSL, etc.). Le chiffrement doit être garanti 256 bits minimum sur les navigateurs compatibles. Le suivi des recommandations de l’ANSSI doit être respecté.

**SECINF40** : 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 doit être mis en place par le candidat.

Les conditions de journalisation (nature des informations, durée de conservation, modalités d’exploitation, etc.) doivent être fixées conjointement par les deux parties.

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.

**SECINF41** : 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 hébergeur 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.).

# TELEMAINTENANCE

## Généralités

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 dont il dispose ;

**TELEMAIN1 :** L’EFS interdit strictement toute récupération de Données à Caractère Personnel (DCP[[2]](#footnote-2)) ou données de santé

**TELEMAIN2 :** Tout prélèvement de données, hors 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

## 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.

## Télémaintenance

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

**TELEMAIN6 :** 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

**TELEMAIN7 :** Tout accès fera l’objet d’une demande d’approbation par le métier au moment de la connexion par le tiers.

**TELEMAIN8 :** Tout accès sera tracé (horodatage de la connexion et des actions réalisées par le tiers).

**TELEMAIN9 :** Le formulaire d’habilitation transmis par l’EFS devra être dûment complété par le tiers avant la création d’un accès en télémaintenance.

**TELEMAIN10 :** Tout compte d’accès doit être nominatif et fera l’objet d’une fiche d’habilitation individuelle.

**TELEMAIN11**: Le tiers s’engage à informer sans délai l’EFS en cas mouvement de personnel.

**TELEMAIN12 :** 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.

**TELEMAIN13 :** Le tiers devra procéder à une revue d’habilitation annuelle des comptes actifs ;

**TELEMAIN14 :** L’EFS se réserve le droit de couper, sans préavis, son accès internet en cas de force majeure.

**TELEMAIN15 :** 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.

**TELEMAIN16 :** L’accès distant ne sera permis que depuis des plages d’adresses IP déclarées par le télémainteneur.

## maintenance PREDICTIVE

**TELEMAIN17 :** 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

**TELEMAIN18 :** L’EFS se réserve le droit d’auditer le trafic entre l’automate et le serveur distant

**TELEMAIN19 :** 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

**TELEMAIN20 :** L’EFS se réserve le droit de couper son accès internet en cas de force majeure.

# RELATIONS AVEC LES TIERS

**RELSTIERS1 :** Le candidat 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 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 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 référentiel.

**RELSTIERS4 :** Le candidat 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 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 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-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.

# 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 la convention de service :

- 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.

**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.

# Plan de Continuité d’activité

**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.

# PLAN d’ASSURANCE sécurité (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.

# Audits de sécurité

**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 devront 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

Cocher la case correspondante *CONFORME* ou *NON-CONFORME*.

Indiquer dans la colonne *OBSERVATIONS*, **la référence du document/paragraphe** traitant l’exigence dans la réponse au besoin. Nous faire parvenir l’ensemble de la documentation citée.

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** |  |  |  |
| **SECURITE INFORMATIQUE** | **SECINF1** |  |  |  |
| **SECINF2** |  |  |  |
| **SECINF3** |  |  |  |
| **SECINF4** |  |  |  |
| **SECINF5** |  |  |  |
| **SECINF6** |  |  |  |
| **SECINF7** |  |  |  |
| **SECINF8** |  |  |  |
| **SECINF9** |  |  |  |
| **SECINF10** |  |  |  |
| **SECINF11** |  |  |  |
| **SECINF12** |  |  |  |
| **SECINF13** |  |  |  |
| **SECINF14** |  |  |  |
| **SECINF15** |  |  |  |
| **SECINF16** |  |  |  |
| **SECINF17** |  |  |  |
| **SECINF18** |  |  |  |
| **SECINF19** |  |  |  |
| **SECINF20** |  |  |  |
| **SECINF21** |  |  |  |
| **SECINF22** |  |  |  |
| **SECINF23** |  |  |  |
| **SECINF24** |  |  |  |
| **SECINF25** |  |  |  |
| **SECINF26** |  |  |  |
| **SECINF27** |  |  |  |
| **SECINF28** |  |  |  |
| **SECINF29** |  |  |  |
| **SECINF30** |  |  |  |
| **SECINF31** |  |  |  |
| **SECINF32** |  |  |  |
| **SECINF33** |  |  |  |
| **SECINF34** |  |  |  |
| **SECINF35** |  |  |  |
| **SECINF36** |  |  |  |
| **SECINF37** |  |  |  |
| **SECINF38** |  |  |  |
| **SECINF39** |  |  |  |
| **SECINF40** |  |  |  |
| **SECINF41** |  |  |  |
| **TELEMAINTENANCE** | **TELEMAIN1** |  |  |  |
| **TELEMAIN2** |  |  |  |
| **TELEMAIN3** |  |  |  |
| **TELEMAIN4** |  |  |  |
| **TELEMAIN5** |  |  |  |
| **TELEMAIN6** |  |  |  |
| **TELEMAIN7** |  |  |  |
| **TELEMAIN8** |  |  |  |
| **TELEMAIN9** |  |  |  |
| **TELEMAIN10** |  |  |  |
| **TELEMAIN11** |  |  |  |
| **TELEMAIN12** |  |  |  |
| **TELEMAIN13** |  |  |  |
| **TELEMAIN14** |  |  |  |
| **TELEMAIN15** |  |  |  |
| **TELEMAIN16** |  |  |  |
| **TELEMAIN17** |  |  |  |
| **TELEMAIN18** |  |  |  |
| **TELEMAIN19** |  |  |  |
| **TELEMAIN20** |  |  |  |
| **RELATIONS AVEC LES TIERS** | **RELSTIERS1** |  |  |  |
| **RELSTIERS2** |  |  |  |
| **RELSTIERS3** |  |  |  |
| **RELSTIERS4** |  |  |  |
| **RELSTIERS5** |  |  |  |
| **RELSTIERS6** |  |  |  |
| **FIN DU CONTRAT** | **FINCONTR1** |  |  |  |
| **FINCONTR2** |  |  |  |
| **FINCONTR3** |  |  |  |
| **PLAN DE CONTINUITE D’ACTIVITE** | **PCA1** |  |  |  |
| **PLAN D’ASSURANCE SECURITE** | **PASSEC1** |  |  |  |
| **PASSEC2** |  |  |  |
| **PASSEC3** |  |  |  |
| **AUDITS DE SECURITE** | **AUDSEC1** |  |  |  |
| **AUDSEC2** |  |  |  |
| **AUDSEC3** |  |  |  |
| **AUDSEC4** |  |  |  |
| **AUDSEC5** |  |  |  |
| **AUDSEC6** |  |  |  |
| **AUDSEC7** |  |  |  |

1. 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]

   . [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)