

# Exigences de Sécurité des Systèmes d'Information (SSI)

## SC2949 Qualité et Géolocalisation des adresses postales

### HISTORIQUE DES VERSIONS

VERSION	DATE	OBSERVATIONS	REDACTEUR	VERIFICATEUR	APPROBATEUR
3.0	26/03/2025	Ajout des exigences de maintenance : <b>MAINTEN 1 à MAINTEN 14</b>	Maricela Pélegrin-Bomel RNSSI		

### SOMMAIRE

<b>1. INTRODUCTION</b>	3
<b>2. SECURITE ORGANISATIONNELLE</b>	4
<b>3. SECURITE PHYSIQUE DES LOCAUX</b>	4
3.1. EXPOSITION AUX RISQUES	4
3.2. REFERENTIELS APPLICABLES	4
3.3. PROTECTION CONTRE L'INTRUSION	5
3.4. TELESURVEILLANCE	5
3.5. SECURITE INCENDIE	5
3.6. PROTECTION CONTRE LES DEGATS DES EAUX	5
3.7. MAINTIEN EN CONDITIONS OPERATIONNELLES DES EQUIPEMENTS DE SECURITE	6
<b>4. SECURITE INFORMATIQUE</b>	6
4.1. GENERALITES	6
<b>5. RELATIONS AVEC LES TIERS</b>	8
<b>6. FIN DU CONTRAT</b>	9
<b>7. PLAN DE CONTINUITE D'ACTIVITE</b>	9
<b>8. PLAN D'ASSURANCE SECURITE (PAS)</b>	9
<b>9. AUDITS DE SECURITE</b>	10
<b>ANNEXE 1 : MATRICE DE CONFORMITE</b>	11

## **GLOSSAIRE :**

<b>AES</b>	<i>Advanced Encryption Standard</i>
<b>ANSSI</b>	Agence Nationale de Sécurité des Systèmes d'Information
<b>APSAD</b>	Assemblée Plénière des Sociétés d'Assurance Dommage
<b>EFS</b>	Etablissement Français du Sang
<b>PAS</b>	Plan d'Assurance Sécurité
<b>PCA</b>	Plan de Continuité d'Activité
<b>Prescripteur</b>	Client Interne de l'EFS
<b>RGS</b>	Référentiel Général de Sécurité
<b>RGPD</b>	Le règlement général sur la protection des données
<b>RNSSI</b>	Responsable National de la Sécurité des Systèmes d'Information
<b>SAAS</b>	<i>Software as a service</i> <sup>1</sup> (Logiciel en tant que service)
<b>SI</b>	Systèmes d'Information
<b>SSI</b>	Sécurité des Systèmes d'Information

---

<sup>1</sup> 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 est invité 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 doit garder à l'esprit que la non-conformité n'est pas un blocage pour devenir le candidat et participer à cette consultation. Le candidat 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.
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 <b>uniquement si le candidat devient le Candidat</b> du service

En réponse à nos exigences il est impératif de :

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

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

## 2. SECURITE ORGANISATIONNELLE

---

**SECORG1** : Le candidat 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 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 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 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 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 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 doit obligatoirement faire appliquer les exigences de sécurité à l'ensemble des sous-traitants participant à la délivrance du service.

## 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 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 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 candidat .

**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 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 APSAD<sup>2</sup>.

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

**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 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.

---

<sup>2</sup> Assemblée Plénière de Sociétés d'Assurances Dommages

**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 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 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** : 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.

**SECINF5** : 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.

**SECINF6** : 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.

**SECINF7** : Les fichiers de l'EFS ne doivent pas être dupliqués ni transmis à un tiers sans l'accord de l'EFS.

**SECINF8** : 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.

**SECINF9** : 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.

**SECINF10** : 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.

**SECINF11** : Les mots de passe des utilisateurs doivent être changés au moins tous les 3 mois.

**SECINF12** : 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 candidat .

**SECINF13** : 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.

**SECINF14** : Les moyens d'authentification incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

**SECINF15** : 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.

**SECINF16** : Les traces doivent pouvoir être imputables à un individu. Elles sont horodatées selon une référence horaire commune à l'ensemble de l'entreprise.

**SECINF17** : 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.

**SECINF18** : 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 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.

**SECINF19** : 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.

**SECINF20** : 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 mise en place par le candidat ou 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.

**SECINF21** : 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 :

- 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.).

**SECINF22** : Le candidat 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 Candidat et la RNSSI de l'EFS.

**SECINF23** : Le candidat doit maintenir à jour ses équipements réseau, ses systèmes d'exploitation et ses applications avec les derniers correctifs de sécurité.

**SECINF24** : Le candidat 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.

**SECINF25** : Le candidat doit effectuer des analyses régulières des vulnérabilités pour identifier et corriger les failles de sécurité.

**SECINF26** : Le candidat 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.

**SECINF27** : Le candidat doit utiliser des protocoles de routage sécurisés pour empêcher les attaques d'usurpation ou de détournement.

## 5. 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 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 document.

**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-divulgence vis-à-vis des tiers participant à la mise en œuvre du service.

## 6. FIN DU CONTRAT

---

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

**FINCONTR3** : Le candidat 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.

## 7. 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.

## 8. PLAN D'ASSURANCE SECURITE (PAS)

---

**PASSEC1** : Une fois la fin de la consultation et le choix d'un candidat , 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 de respecter le niveau minimal de sécurité.**

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

**PASSEC3** : Un tableau de bord indiquant l'état de la conformité des exigences de sécurité doit être fourni par le candidat à une fréquence définie en commun accord entre le RSSI du candidat et le RNSSI de l'EFS. Si des écarts sont constatés, le candidat 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.

## 9. AUDITS DE SECURITE

---

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

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

## ANNEXE 1 : MATRICE DE CONFORMITE

Comment remplir cette matrice

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

DOMAINES	REFERENCE EXIGENCE	CONFORME	NON-CONFORME	OBSERVATIONS
SECURITE ORGANISATIONNELLE	SECORG1			
	SECORG2			
	SECORG3			
	SECORG4			
	SECORG5			
	SECORG6			
	SECORG7			
	SECORG8			
SECURITE PHYSIQUE DES LOCAUX	SECPHY-ER1			
	SECPHY-RA1			
	SECPHY-PL1			
	SECPHY-PL2			
	SECPHY-PL3			
	SECPHY-PL4			
	SECPHY-TSV1			
	SECPHY-SI1			
	SECPHY-SI2			
	SECPHY-SI3			
	SECPHY-SI4			
	SECPHY-SI5			
	SECPHY-PGE1			
	SECPHY-PGE2			
	SECPHY-PGE3			
	SECPHY-PGE4			
	SECPHY-PGE5			
	SECPHY-MCO1			
	SECPHY-MCO2			
	SECPHY-MCO3			
	SECPHY-MCO4			
	SECPHY-MCO5			
	SECINF1			

SECURITE INFORMATIQUE	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			
RELATIONS AVEC LES TIERS	RELSTIERS1			
	RELSTIERS2			
	RELSTIERS3			
	RELSTIERS4			
	RELSTIERS5			
	RELSTIERS6			
FIN DU CONTRAT	FINCONTR1			
	FINCONTR2			
	FINCONTR3			
	FINCONTR4			
PLAN DE CONTINUITE D'ACTIVITE	PCA1			
PLAN D'ASSURANCE SECURITE	PASSEC1			
	PASSEC2			
	PASSEC3			
AUDITS DE SECURITE	AUDSEC1			
	AUDSEC2			

	AUDSEC3			
	AUDSEC4			
	AUDSEC5			
	AUDSEC6			
	AUDSEC7			