

Matrice des exigences de sécurité des systèmes d'information (SSI) pour le titulaire de l'EFS dans le cadre du marché fourniture de réactifs pour l'étude du chimérisme technique sensible de RQ-PCR

HISTORIQUE DES VERSIONS

VERSION	DATE	OBSERVATIONS	REDACTEUR	VERIFICATEUR	APPROBATEUR
2.15	11/09/2023	<p>Changement des exigences :</p> <ul style="list-style-type: none"> - SECINF16 : Les mots de passe des comptes utilisés par les applications doivent être constitués d'au moins 16 caractères alphanumériques - SAAS CRYPTO-3 <p>Si le protocole <i>Transport Layer Security</i> (TLS) est mis en œuvre, le titulaire doit appliquer les recommandations de l'ANSSI relatives à TLS,</p>	Maricela Pélegrin-Bomel RNSSI		
2.16	26/10/2023	<ul style="list-style-type: none"> • Modification de l'exigence SECINF14 : Les mots de passe des utilisateurs doivent être changés au moins tous les 3 mois et doivent comporter au minimum 12 caractères alphanumériques • Ajout d'exigences pour les aspects réseaux. : SECINF36 à SECINF40 	Maricela Pélegrin-Bomel RNSSI		

2.17	4/12/2023	<p>: 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 :</p> <ul style="list-style-type: none"> • 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. <p>Dans le cadre des administrateurs ceux derniers doivent suivre les règles suivantes :</p> <ul style="list-style-type: none"> • 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 	Maricela Pélegrin-Bomel RNSSI		
2.18	29/05/2024	Mise à jour du bas de page sur la Circulaire du Cloud au Centre : 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]	Maricela Pélegrin-Bomel RNSSI		

SOMMAIRE

1. INTRODUCTION	5
2. SECURITE ORGANISATIONNELLE	6
3. SECURITE PHYSIQUE DES LOCAUX	6
4. SECURITE INFORMATIQUE	7
4.1. GENERALITES	7
4.2. RELATIONS AVEC LES TIERS	7
4.3. INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION	8
4.4. FIN DU CONTRAT	8
5. PLAN DE CONTINUITE D'ACTIVITE	8
6. PLAN D'ASSURANCE SECURITE (PAS)	8

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
RNSSI	Responsable National de la Sécurité des Systèmes d'Information
SAAS	SAAS Software as a service 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, et le plan de continuité d'activité y sont présentés.

Les candidats et/ou titulaires 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 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. 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.
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 Titulaire doit présenter une politique de sécurité formalisée dont le périmètre couvre les risques de continuité de service et de malveillance auxquels il est exposé au titre de la prestation.

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

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

SECORG4 : 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.

SECORG5 : Le titulaire doit sensibiliser à la sécurité de l'information et aux risques liés à la protection des données l'ensemble des personnes impliquées dans la fourniture du service.

SECORG6 : Le Titulaire doit obligatoirement faire appliquer les exigences de sécurité à l'ensemble des sous-traitants participant à la délivrance du service.

SECORG7 : Le titulaire 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

3.1. SECURITE PHYSIQUE 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 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 : En cas d'expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le 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 la continuité du service fourni par le titulaire dans les meilleures conditions (transfert de compétence, documents explicatifs, etc.).

SECINF4 : 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.

SECINF5 : Le titulaire doit maintenir à jour ses équipements réseau, ses systèmes d'exploitation et ses applications avec les derniers correctifs de sécurité.

SECINF6 : Le titulaire doit effectuer des analyses régulières des vulnérabilités pour identifier et corriger les failles de sécurité.

4.2. RELATIONS AVEC LES TIERS

SECINF-RELSTIERS1 : Le titulaire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le titulaire doit inclure ces exigences dans les contrats conclus avec les tiers.

SECINF -RELSTIERS2 : Le titulaire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent document.

SECINF -RELSTIERS3 : Le titulaire doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

SECINF-RELSTIERS4 : Le titulaire doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences de ce recueil d'exigences. **SECINF-RELSTIERS5** : Le titulaire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgence vis-à-vis des tiers participant à la mise en œuvre du service.

4.3. INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION

SECINF-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, et que cela impacte la livraison des réactifs à l'EFS, 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.

4.4. FIN DU CONTRAT

SECINF-FINCONTR1 : À la fin du contrat liant le titulaire et le commanditaire, que le contrat soit arrivé à son terme ou ur toute autre cause, le titulaire doit assurer un effacement sécurisé par réécriture de motifs aléatoires tout support de données mis à disposition du commanditaire. Si l'espace de stockage est chiffré, l'effacement peut être réalisé par un effacement sécurisé de la clé de chiffrement.

SECINF-FINCONTR2 : La suppression des données ne pourra être réalisée qu'une fois la réversibilité finalisée et un procès-verbal signé par le client.

5. 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.

6. PLAN D'ASSURANCE SECURITE (PAS)

PASSEC1 : le Titulaire doit produire 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 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.

