

ACHAT d'un système de gestion de salle d'azote destiné au site EFS de BESANÇON et prestations associées

Annexe 2 CCTP

Exigences de Sécurité des Systèmes d'Information (SSI) à l'EFS

SOMMAIRE

1. INTRODUCTION	4
2. SECURITE ORGANISATIONNELLE	5
3. SECURITE PHYSIQUE DES LOCAUX	5
3.1. EXPOSITION AUX RISQUES	5
3.2. REFERENTIELS APPLICABLES.....	5
3.3. PROTECTION CONTRE L'INTRUSION	6
3.4. TELESURVEILLANCE	6
3.5. SECURITE INCENDIE	6
3.6. PROTECTION CONTRE LES DEGATS DES EAUX	6
3.7. MAINTIEN EN CONDITIONS OPERATIONNELLES DES EQUIPEMENTS DE SECURITE	7
4. SECURITE INFORMATIQUE	7
4.1. GENERALITES	7
5. TELEMANTENANCE	10
5.1. GENERALITES	10
5.2. TELEMANTENANCE	10
6. RELATIONS AVEC LES TIERS	11
7. PLAN DE CONTINUITE D'ACTIVITE	11
8. PLAN D'ASSURANCE SECURITE (PAS)	11
ANNEXE 1 : MATRICE DE CONFORMITE	13

GLOSSAIRE :

AES	Advanced Encryption Standard
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 Titulaire d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le Titulaire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application

1. INTRODUCTION

L'Etablissement Français du Sang (EFS), est conscient de sa mission en tant qu'opérateur unique de la transfusion sanguine en France mais aussi de son obligation de protéger les données personnelles de ses donneurs, les receveurs et de son personnel.

A ce titre, l'EFS doit assurer la continuité de la transfusion sanguine en France et se doit de vérifier que les activités confiées à des tiers partenaires ou à des sous-traitants se déroulent dans le respect des conditions de disponibilité, intégrité et confidentialité, fiabilité et authentification imposées par les obligations légales de son activité dépendante de son système d'information.

Le présent document comporte les exigences de Sécurité des Systèmes d'Information de l'EFS applicables aux prestations prévues au marché. Les volets relatifs à la sécurité organisationnelle, la sécurité 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 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. Les exigences de cette partie concerne la maintenance du matériel et du logiciel qui s'y rattache et ne concerne pas les applications utilisateurs.
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 Titulaire doit présenter une politique de sécurité formalisée dont le périmètre couvre les risques de continuité de service et de malveillance auxquels il est exposé au titre de la prestation.

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

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

SECORG4 : Tout collaborateur du Titulaire participant à l'activité de l'EFS doit respecter les procédures et les règles de sécurité applicables dans le cadre de la réalisation de la prestation.

SECORG5 : Tout collaborateur du Titulaire participant à l'activité de l'EFS doit avoir signé un engagement personnel de confidentialité dans le cadre de son contrat de travail.

SECORG6 : Le Titulaire doit documenter et mettre en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.

SECORG7 : Le Titulaire doit sensibiliser à la sécurité de l'information et aux risques liés à la protection des données l'ensemble des personnes impliquées dans la fourniture du service.

SECORG8 : Le Titulaire doit obligatoirement faire appliquer les exigences de sécurité à l'ensemble des sous-traitants participant à la délivrance du service.

3. SECURITE 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 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 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 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 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.

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 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.

² 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 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 Titulaire mettra en œuvre les mesures de sécurité suivantes :

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

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

SECINF3 : 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

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 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.

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 exécutables de l'EFS ne doivent pas être dupliqués ni transmis à un tiers sans l'accord de l'EFS.

SECINF7 : Les exécutables 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.

SECINF8 : 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.

SECINF9 : 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.

SECINF10 : En cas de nécessité (requête des autorités, cas de malveillance, ...), le Titulaire 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 ans.

SECINF12 : Les mots de passe des comptes utilisés par les applications et les traitements automatisés doivent être changés au moins tous les ans. Ils ne doivent être accessibles et modifiables que par l'exploitant de ce traitement.

SECINF13 : La résistance des mots de passe est suivie et contrôlée de façon à ce que ceux-ci ne soient pas devinables, c'est-à-dire qu'ils ne sont pas une dérivation simple du login de l'utilisateur, de son nom, de son prénom, d'une date, d'un nom commun, d'un prénom ou d'un nom propre en langue française, anglaise ou de celle du pays dans lequel sont implantés les locaux du Titulaire.

SECINF14 : 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.

SECINF15 : Les moyens d'authentification incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

SECINF16 : 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.

SECINF17 : Les traces doivent pouvoir être imputables à un individu. Elles sont horodatées selon une référence horaire commune à l'ensemble de l'entreprise.

SECINF18 : Les informations auxquelles le titulaire pourrait accéder dans le cadre de sa prestation

sont strictement confidentielles et le titulaire s'engage à ne pas les diffuser sous aucune forme. De plus, il doit s'assurer du respect par ses collaborateurs du document « *Habilitation* ». Celui-ci devra être signé par les collaborateurs concernés. Une liste des habilitations signées doit être adressée annuellement auprès des responsables de la prestation de l'EFS.

SECINF19 : Les sauvegardes des sources informatiques sont faites régulièrement et traitées de manière à garantir leur disponibilité, confidentialité et leur intégrité. Les sauvegardes des sources devront être effectuées sur un site différent et distant.

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

SECINF21 : 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, ...).

SECINF22 : Le 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 le Prescripteur, elles doivent être stockées de manière chiffrée et répliquées à intervalles réguliers dans la journée.

SECINF23 : 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 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.

SECINF24 : En cas d'expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le 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.).

SECINF25 : Lorsqu'il est mis fin à l'hébergement, le 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.

SECINF26 : Le Titulaire doit assurer la traçabilité des incidents de sécurité des systèmes d'information et prévenir le RNSSI de l'EFS et le responsable de la relation, au DSIM. 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

³ Circulaire du Premier ministre n° 6282 SG du 5 juillet 2021 sur la doctrine de l'utilisation de l'informatique au nuage par l'Etat (« Cloud au centre »)

Puis Doctrine Cloud au Centre du 15/09/2021 de Nadi BOU HANNA Directeur Interministériel du Numérique. Fait référence à la Règle 9 de la circulaire 6282-SG du 5 juillet 2021, relative à l'utilisation de l'informatique en nuage de l'Etat. Tout système numérique manipulant des données sensibles ne doit pas utiliser les services Microsoft et Office 365. Obligation de prendre la position **Cloud au Centre** c'est à dire opérateur avec Visa SecNumCloud de l'ANSSI et immunisée contre les réglementations extracommunautaires.

remettre à niveau la ou les exigences et cela en commun accord entre le RSSI du Titulaire et la RNSSI de l'EFS.

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

SECINF28 : Le Titulaire doit 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.

SECINF29 : Le Titulaire doit utiliser des protocoles de routage sécurisés pour empêcher les attaques d'usurpation ou de détournement.

5. TELEMAINTENANCE

5.1. GENERALITES

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 maintenance :

TELEMAIN1 : L'EFS interdit strictement toute récupération de Données à Caractère Personnel (DCP⁴) 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 Titulaire 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

5.2. TELEMAINTENANCE

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 équipements 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 DSIM 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.

⁴ 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.

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 48 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.

6. RELATIONS AVEC LES TIERS

RELSTIERS1 : Le Titulaire doit tenir à disposition du commanditaire la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de sous-traitants au sens de l'article 28 du [RGPD] afin que le commanditaire puisse émettre des objections à cet égard.

RELSTIERS2: Le Titulaire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le Titulaire doit inclure ces exigences dans les contrats conclus avec les tiers.

RELSTIERS3 : Le Titulaire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent référentiel.

RELSTIERS4 : Le Titulaire doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

7. PLAN DE CONTINUITE D'ACTIVITE

PCA1 : Un plan de continuité d'activité concernant l'outil, formalisé et testé doit permettre de prévenir ou de subvenir à toute panne grave ou à tout sinistre de votre système d'information impactant les obligations définies dans le Contrat.

Ce plan de continuité assure à minima la sauvegarde régulière de l'application.

8. PLAN D'ASSURANCE SECURITE (PAS)

PASSEC1 : Le Titulaire 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 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.

9. FIN DU CONTRAT

FINCONTR1 : À la fin du contrat liant le Titulaire et le commanditaire, que le contrat soit arrivé à son terme ou pour toute autre cause, le Titulaire doit assurer un effacement sécurisé de l'intégralité des données du commanditaire. Cet effacement doit être réalisé par réécriture complète de tout support ayant hébergé ces données et ce dans un délai précisé dans la convention de service.

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

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			
	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			
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			
TELEMAINTENANCE	TELEMAIN1			
	TELEMAIN2			
	TELEMAIN3			
	TELEMAIN4			
	TELEMAIN5			
	TELEMAIN6			
	TELEMAIN7			
	TELEMAIN8			
	TELEMAIN9			
	TELEMAIN10			
	TELEMAIN11			
	TELEMAIN12			
	TELEMAIN13			
	TELEMAIN14			
	TELEMAIN15			
	TELEMAIN16			

RELATIONS AVEC LES TIERS	RELSTIERS1			
	RELSTIERS2			
	RELSTIERS3			
	RELSTIERS4			
PLAN DE CONTINUITE D'ACTIVITE	PCA1			
PLAN D'ASSURANCE SECURITE	PASSEC1			
	PASSEC2			
	PASSEC3			
FIN DU CONTRAT	FINCONTR1			
	FINCONTR2			