

ENTÊTE RÉSERVÉE : MERCI DE NE RIEN INSCRIRE

Version	Date	Rédacteur	M – Modifié A – Ajouté S – Supprimé	Nature de l'évolution
1	10/10/2022	B.BOUDIBA -RSSI	A	Création du document – mise en conformité documentaire
1.2	06/11/2023	B.BOUDIBA -RSSI	M	Ajout chapitre 6.14 services hébergés et Cloud
1.3	06/11/2023	B.BOUDIBA -RSSI	M	Prise en compte des remarques DPO et Service Achat
1.4	15/11/2023	B.BOUDIBA -RSSI	M	Prise en compte des remarques du Service Achat
1.5	21/02/2024	B.BOUDIBA -RSSI	M	MAJ remarques du Service Achat : RAF Maj exception Recherche

Sommaire

1. Objet	4
2. Domaine d'application	4
3. Référence(s) et document(s) annexe(s).....	4
3.1. Référence(s)	4
3.1.1. Références documents internes.....	4
3.1.2. Références externes.....	4
3.2. Document(s) annexe(s)	4
4. Définitions et abréviations.....	4
5. Responsabilités et personnes ressources	5
5.1. Responsabilités.....	5
5.2. Personnes ressources.....	5
6. Contenu	5
6.1. Infrastructures et télémaintenance	5
6.2. Organisation de la sécurité de l'information.....	6
6.3. La sécurité des ressources humaines.....	6
6.4. Gestion des actifs	6
6.4.1. Responsabilités relatives aux actifs	6
6.4.2. Classification de l'information	7
6.4.3. Manipulation des supports	7

6.5. Contrôle d'accès	7
6.5.1. Exigences en matière de contrôle d'accès	7
6.5.2. Gestion de l'accès utilisateur.....	8
6.5.3. Responsabilités des utilisateurs.....	8
6.5.4. Contrôle de l'accès au système et aux applications.....	8
6.6. Cryptographie	9
6.7. Sécurité physique et environnementale	9
6.7.1. Zones sécurisées	9
6.7.2. Matériels	9
6.8. Sécurité liée à l'exploitation.....	10
6.8.1. Procédures et responsabilités liées à l'exploitation.....	10
6.8.2. Protection contre les logiciels malveillants.....	10
6.8.3. Sauvegarde	10
6.8.4. Journalisation et surveillance	11
6.8.5. Maîtrise des logiciels en exploitation	11
6.8.6. Gestion des vulnérabilités techniques	11
6.9. Sécurité des communications	11
6.9.1. Management de la sécurité des réseaux.....	11
6.9.2. Transfert de l'information.....	12
6.10. Conformité	12
6.11. Acquisition, développement et maintenance des systèmes d'information	12
6.11.1. Exigences de sécurité applicables aux systèmes d'information.....	12
6.11.2. Sécurité des processus de développement et d'assistance technique.....	12
6.11.3. Données de test.....	13
6.12. Gestion des incidents liés à la sécurité de l'information.....	13
6.13. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	14
6.14. Cas de service hébergé en dehors du SI du bénéficiaire et de prestation de type Cloud Saas/Iaas et infogérance dans le SI du bénéficiaire	14
6.14.1. Accès par des utilisateurs du bénéficiaire au service hébergé	14
6.14.2. Continuité du service hébergé.....	15
6.14.3. Réversibilité du service hébergé.....	15

6.14.4. Garantie de Confidentialité des données hébergées	15
6.14.5. Solution est installée dans l'infrastructure informatique du bénéficiaire mais administrée intégralement par le titulaire	15
6.14.6. Perte ou le renouvellement de certification d'hébergement de données de santé	16

1. Objet

Ce document est une annexe au cahier des clauses techniques particulières destiné aux fournisseurs.

L'intégration systématique de cette annexe est nécessaire dès lors qu'il y a une interconnexion avec le système d'information du GHT Sud Lorraine ou dans le cas où le titulaire pourrait accéder, traiter, stocker, manipuler des données sensibles ou fournir des composants d'infrastructure informatique.

Les exigences spécifiques de service hébergé en dehors du Système d'Information (SI) du bénéficiaire et de prestation hébergée dans le Cloud sont précisées au paragraphe « Cas de service hébergé en dehors du SI du bénéficiaire et de prestation de type Cloud Saas/Iaas et infogérance dans le SI du bénéficiaire » de ce document.

2. Domaine d'application

Les directives de sécurité prises en compte par l'annexe au cahier des clauses techniques particulières concernent les fournisseurs.

3. Référence(s) et document(s) annexe(s)

3.1. Référence(s)

3.1.1. *Références documents internes*

- Politique de sécurité des systèmes d'information (PSSI)

3.1.2. *Références externes*

- ISO 27002 : 2017

3.2. Document(s) annexe(s)

Néant.

4. Définitions et abréviations

- CCTP** : Cahier des Clauses Techniques Particulières
- Titulaire** : Le titulaire est le fournisseur, ou le prestataire de services, qui conclut le marché avec la personne morale de droit public.

5. Responsabilités et personnes ressources

5.1. Responsabilités

- Les personnes responsables de l'application de ce document sont les adjoints du DTNIB ainsi que le Responsable de la Sécurité du Système d'Information (RSSI).

5.2. Personnes ressources

Pour tout renseignement en rapport avec le contenu de ce document vous pouvez contacter les référents et rédacteurs.

6. Contenu

6.1. Infrastructures et télémaintenance

La mise en place de demande de machine virtuelles sur le Système d'Information du CHRU de Nancy devra respecter les éléments de sécurité en vigueur au même titre que les postes de travail. La solution devra obligatoirement respecter les consignes suivantes qui devront être appliquées avant toute mise en production :

- L'éditeur ou l'intégrateur définira les caractéristiques techniques en termes d'OS (Système d'exploitation), de prérequis et de dimensionnement des machines virtuelles qui seront nécessaire. Seuls les OS à jour et supportés par les éditeurs sont autorisés.
- Le système de gestion et de prise de main à distance ainsi que l'antivirus et l'EDR du CHRU de Nancy seront installés.
- L'ensemble des patchs de sécurité OS seront appliqués à minima mensuellement via les outils du CHRU de Nancy.
- L'ensemble des accès réseaux sont fermés par défaut et seront à définir précisément pour validation et ouverture.
- Les comptes utilisateurs ou applicatifs seront à demander avec les droits associés qui bénéficieront des privilèges minimaux nécessaires.
- Aucun compte générique ou session restant active ne sera autorisé.
- Tous les protocoles d'accès et d'échanges devront être chiffrés et sécurisés.
- Le CHRU de Nancy est en capacité de fournir, en fonction des capacités applicatives, des machines redondées sur deux DataCenter et de réaliser des sauvegardes des systèmes.
- Les accès extérieurs entrants ou sortants passeront obligatoirement de manière authentifiée avec inspection via les infrastructures Proxy et VPN du CHRU de Nancy.
- Les accès en télémaintenance feront l'objet d'un engagement contractuel et d'une ouverture sur appel au Centre de Service. De plus une authentification MFA (multi-facteurs) sera imposée.

Tout équipement Wi-Fi à intégrer au Système d'Information devra respecter l'ensemble des règles en vigueur au CHRU de Nancy :

- Utilisation des réseaux SSID en place et cachés, aucun réseau dédié ne sera créé
- Utilisation de la sécurité WPA2 AES authentification EAP via ISE Cisco
- Suivi des évolutions techniques en termes de bande de fréquence et protocoles
- Si une étude de couverture complémentaire doit être réalisée, et une extension prévue, celle-ci doit être prévue dans le cadre du projet ou spécifiquement indiqué.

6.2. Organisation de la sécurité de l'information

Le titulaire met en œuvre une organisation de sécurité de l'information et alloue les ressources nécessaires à la définition des responsabilités, au cloisonnement des tâches, à la mise en œuvre des actions de sécurité physiques et logiques et rend compte au bénéficiaire des éventuels incidents.

Le titulaire s'engage sur les mesures nécessaires à la sécurisation des postes de travail et des équipements mobiles utilisés par ses personnels et ses sous-traitants dans l'exécution du contrat afin que ces équipements ne constituent pas un vecteur d'atteinte à la sécurité de l'information ; notamment par une limitation de l'accès aux données (chiffrement des équipements, verrouillage automatique de session ...).

6.3. La sécurité des ressources humaines

Le titulaire s'engage à s'assurer que les personnels affectés aux travaux relatifs à l'exécution du marché ont les niveaux de connaissances et de compétences techniques requis pour la réalisation des tâches qui leur sont confiées.

Le titulaire veille à faire respecter les règles de sécurité et de confidentialité avant le démarrage des services, en faisant signer un accord de confidentialité ou en prévoyant une clause dans le contrat de travail. Les obligations de l'accord de confidentialité doivent s'étendre au-delà de la fin de la prestation contractuelle.

6.4. Gestion des actifs

6.4.1. Responsabilités relatives aux actifs

Le titulaire dispose et tient à jour un inventaire des actifs informatiques où sont traitées les données du bénéficiaire. Cet inventaire consigne les informations suivantes : propriétaire, nom du serveur, localisation et la configuration.

En cas d'échéance ou de résiliation du marché, le titulaire s'engage :

- À permettre au bénéficiaire de récupérer de façon sécurisée une copie de l'intégralité des données (réversibilité) dans un format exploitable par le bénéficiaire. Cette restitution des données ainsi que leur exploitabilité par le bénéficiaire et constatée par procès-verbal daté et signé par le bénéficiaire.
- Une fois le procès-verbal signé, à détruire les copies des données détenues dans ses systèmes informatiques et à en apporter la preuve au bénéficiaire dans un délai convenu entre les Parties. Les données « actives » (dont l'accès est fréquent) disponibles en ligne sont effacées immédiatement ; les données « froides » (dont l'accès est rare mais nécessaire) sont effacées dans les meilleurs délais (date butoir convenue avec le bénéficiaire). Cette suppression sera assurée par le biais d'un effacement sécurisé des données du bénéficiaire figurant sur ses équipements et l'ensemble des pans de son système d'information, sans possibilité de reconstitution.

Sur simple demande du bénéficiaire, le titulaire s'engage à permettre un export des données stockées sur ses services dans un format exploitable par le bénéficiaire.

Le titulaire s'engage à ce que ses personnels et sous-traitants impliqués dans l'exécution du marché, restituent la totalité des actifs (ex : documents papiers, ordinateurs, téléphones...) qu'ils ont en leur possession au terme du marché ou de leur période d'emploi.

6.4.2. Classification de l'information

Le titulaire met en place, tient à jour et partage avec le bénéficiaire, une classification des informations (notamment les données à caractère personnel) en termes d'exigences légales, de confidentialité, de sensibilité au regard d'une modification non autorisée.

Le titulaire met en œuvre des mesures de protection proportionnées aux enjeux de sécurité décrits dans la classification.

6.4.3. Manipulation des supports

Le titulaire s'engage à protéger la confidentialité des données sur les médias amovibles (par exemple au moyen du chiffrement), et lors de transferts à des tiers (par exemple au moyen du chiffrement, contrôles d'accès...).

Le titulaire veille à ce que les fichiers temporaires contenant des données confidentielles (notamment les données à caractère personnel) soient définitivement supprimés lorsqu'ils ne sont plus nécessaires à l'exécution du traitement.

Au terme de l'utilisation d'un matériel informatique par le titulaire (notamment en cas de mise au rebut, vente, réattribution ou recyclage) utilisé dans le cadre de la prestation et plus particulièrement pour les matériels de stockage, il ne doit rien rester sur celui-ci qui pourrait entraîner la divulgation d'informations de du bénéficiaire.

6.5. Contrôle d'accès

6.5.1. Exigences en matière de contrôle d'accès

Le titulaire établit, documente et met à jour une politique de contrôle d'accès sur la base des enjeux de sécurité.

Les utilisateurs ont uniquement accès aux ressources informatiques pour lesquelles ils ont reçu

une autorisation.

6.5.2. Gestion de l'accès utilisateur

Le titulaire s'engage également à :

- Réaliser avec une fréquence au moins annuelle la revue des droits, des comptes d'accès et de gestion des anomalies constatées (post réconciliation) assortie de délais sur les environnements utilisés par le bénéficiaire.
- Effectuer avec une fréquence au moins annuelle la revue des comptes utilisateurs et administrateurs qui ne sont pas gérés par le bénéficiaire. En particulier, le titulaire s'engage à s'assurer de la suppression des droits d'accès dès qu'ils ne sont plus justifiés par les besoins de du bénéficiaire.

Le titulaire s'engage à mettre en œuvre, pour son personnel et ses sous-traitants, un contrôle d'accès aux environnements hébergeant les données soumis à une habilitation préalable, en fonction des rôles qui leurs sont attribués et respectant les principes de « moindre privilège » et de « besoin d'en connaître ». A ce titre, le titulaire s'engage à opérer la révocation ou la modification des droits d'accès au Service à chaque changement de statut de son personnel et de ses sous-traitants.

Le titulaire s'engage à respecter la politique de gestion de mot de passe du bénéficiaire.

Le titulaire ne doit stocker que l'empreinte des mots de passe des utilisateurs et des comptes techniques :

- Il doit mettre en œuvre une fonction de hachage toujours conforme aux règles et recommandations énoncées dans la dernière version en vigueur du Référentiel Général de Sécurité de l'ANSSI Annexe B1.
- Il doit générer les empreintes des mots de passe avec une fonction de hachage associée à l'utilisation d'un sel cryptographique toujours conforme aux règles et recommandations énoncées dans la dernière version en vigueur du Référentiel Général de Sécurité de l'ANSSI Annexe B1.

6.5.3. Responsabilités des utilisateurs

Le titulaire met en place une politique de mots de passe :

- Longueur : 12 caractères minimum
- Complexité : au minimum un chiffre, une lettre majuscule, une lettre minuscule, un caractère spécial

Le titulaire diffuse des consignes de sécurité sur la protection des mots de passe auprès de ses utilisateurs.

Le titulaire établit, diffuse et met à jour une procédure en cas de compromission d'un compte

6.5.4. Contrôle de l'accès au système et aux applications

Le titulaire s'engage à mettre en œuvre des dispositifs de séparation garantissant l'étanchéité des environnements utilisateurs et l'isolation des données dans les différents environnements support de son Service et sous toutes leurs formes (stockage, mémoire, transmission, ...). Le titulaire applique une séparation des rôles permettant de ne pas confier un accès et la gestion de la sécurité de cet accès aux mêmes acteurs.

Le titulaire s'engage à cloisonner les environnements de développement, de recette, de production et de secours utilisés par le bénéficiaire.

6.6. Cryptographie

Le titulaire s'engage à mettre en œuvre des méthodes de chiffrement basés sur des standards publics éprouvés conformes avec les exigences du bénéficiaire et à l'Etat de l'art (ANSSI, ENISA, NIST) permettant à toute donnée du bénéficiaire d'être transmise de façon sécurisée à travers un réseau de communication, qu'il soit interne (notamment celui du titulaire) ou public (notamment le réseau Internet). Pour l'établissement de tunnels VPN sécurisés, le titulaire utilisera des moyens et logiciels conformes à l'Etat de l'art. Le titulaire s'engage à mettre en œuvre et à fournir le détail technique et organisationnel des méthodes de chiffrement et de pseudonymisation des données.

Le titulaire s'engage à chiffrer de manière native et systématique les données au repos du bénéficiaire.

Le titulaire s'engage à chiffrer les données lors de leur transfert et en cas de réplication entre ses datacenters. Toutes les solutions utilisées sont basées sur les standards du marché dont le niveau de sécurité est éprouvé.

6.7. Sécurité physique et environnementale

6.7.1. Zones sécurisées

Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.

Les zones sécurisées sont protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.

Le titulaire définit et applique des mesures de sécurité physique aux bureaux, aux salles et aux équipements, en particulier pour se protéger de désastres naturels, d'attaques malveillantes ou les accidents.

6.7.2. Matériels

Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé.

Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage.

Les matériels, les informations ou les logiciels ne doivent pas sortir des locaux de l'organisation sans autorisation préalable.

Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.

Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toutes les données ont bien été supprimées et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.

Les utilisateurs s'assurent que leur ordinateur portable lorsqu'il n'est pas surveillé et doté d'une protection appropriée (par un câble antivol ou mis sous clef). Les utilisateurs verrouillent leur session s'ils quittent leur poste de travail ne serait-ce que quelques instants et éteignent leur ordinateur dès que leur session de travail est terminée.

Une politique du bureau propre pour les documents papier et les supports de stockage amovibles a été définie, communiquée et est appliquée.

6.8. Sécurité liée à l'exploitation

6.8.1. Procédures et responsabilités liées à l'exploitation

Le titulaire doit mettre en œuvre et contrôler les procédures d'exploitation, en particulier celles relatives à la mise à jour des systèmes, aux applications, aux processus d'administration, aux processus de développement et sécurité des développements, à la séparation des environnements de test, de recette et de production.

Le titulaire veille, en particulier, à la sécurité du matériel, des couches d'accès au réseau, des Bases de Données et de leur gestion, des systèmes logiciels réalisant la virtualisation des systèmes. Le titulaire s'engage à mettre en œuvre des systèmes de détection d'intrusion pour faciliter la détection rapide, l'investigation et la réponse aux Incidents de Sécurité.

Le titulaire s'engage à installer les correctifs logiciels le plus tôt possible sur ses applications et ses systèmes. Dans le cas où un correctif aurait un impact sur le niveau de disponibilité et de sécurité de son Service et ses postes de travail.

Le titulaire s'engage à séparer logiquement ou physiquement le réseau d'administration de ses infrastructures de service.

Le titulaire s'engage à mettre en place des procédures et dispositifs pour assurer que les données de production ne sont pas répliquées ou utilisées dans les environnements hors production, et que seules des données fictives (i.e. anonymisées ou fabriquées) sont utilisées à des fins de test ou de recette, sauf demande contraire et expresse du bénéficiaire.

6.8.2. Protection contre les logiciels malveillants

Tous les systèmes disposent de solutions de lutte contre les codes malveillants (ex : anti-malware) ; ces solutions sont installées et mises à jour aussi bien sur les serveurs d'infrastructures que sur les machines d'administration.

6.8.3. Sauvegarde

Une politique de sauvegarde est définie avec le bénéficiaire, précisant la fréquence et la durée de rétention. Les sauvegardes des données stockées sur les moyens du titulaire sont sous la responsabilité de ce dernier. Le titulaire se doit de faire des tests de restauration afin de s'assurer de l'intégrité et du bon fonctionnement de ces sauvegardes.

Le titulaire s'engage sur la mise en place des mesures de protection des médias informatiques

sur lesquels sont enregistrées des données afférentes à la réalisation du marché.

Le titulaire ainsi que ses éventuels Sous-traitants s'engagent à respecter l'Etat de l'art en matière d'effacement sécurisé des différents supports de stockage utilisés dans le cadre des Services.

6.8.4. Journalisation et surveillance

Le titulaire s'engage à mettre en œuvre des capacités de surveillance, de détection et de prévention (ex : sondes IDS/IPS) des traitements non autorisés de l'information, notamment des Violations de données.

Les événements de sécurité détectés sont consignés par le titulaire dans un journal des opérations, de Violations des données et des rapports d'incident auxquels le bénéficiaire doit avoir accès sur demande. Ces rapports sont produits et conservés pendant une période suffisante pour répondre aux contraintes réglementaires du bénéficiaire. Ils doivent respecter la législation en vigueur.

Le contenu de ces traces informatiques doit permettre d'imputer chaque événement journalisé à son origine (personne physique, équipement technique, ...), de dater cet événement et d'en qualifier la nature. Les traces contenant des données à caractère personnel font l'objet d'un suivi particulier.

Le titulaire s'engage à mettre en place des mesures nécessaires à la protection des traces informatiques et notamment à restreindre les accès physiques et logiques, de son personnel et de ses sous-traitants au journal d'événements sécurisés aux seules personnes spécialement habilitées à cet effet.

6.8.5. Maîtrise des logiciels en exploitation

Le titulaire avertit le bénéficiaire avant toute mise à jour d'un composant logiciel de sa plateforme technique.

En cas de livraison d'une évolution majeure du service, le bénéficiaire est en mesure d'exiger un délai.

6.8.6. Gestion des vulnérabilités techniques

Le titulaire a mis en place des procédures permettant d'appliquer des correctifs d'urgence sur son infrastructure de sécurité si une vulnérabilité critique est détectée. A ce titre, le titulaire opère une solution technologique de gestion des vulnérabilités.

6.9. Sécurité des communications

6.9.1. Management de la sécurité des réseaux

Les réseaux sont cloisonnés par le titulaire, entre l'environnement administrateur du titulaire et l'environnement du bénéficiaire.

6.9.2. Transfert de l'information

Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication. L'information transitant par la messagerie électronique doit être protégée de manière appropriée. Les exigences en matière d'engagements de confidentialité ou de non-divulgaration, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.

Lorsque des media amovibles sont utilisés pour des transferts d'information, une procédure est à mettre en place pour enregistrer les entrées et sorties de media contenant des données à caractère personnel (le media concerné, la date et l'heure, les émetteurs et récepteurs autorisés).

L'ensemble des flux doit être chiffré et le protocole HTTPS est systématiquement utilisé avec authentification par certificat des services web.

6.10. Conformité

Le bénéficiaire peut effectuer ou faire effectuer un audit de sécurité auprès du titulaire ou le cas échéant de ses sous-traitants afin de s'assurer de la prise en compte effective du niveau de sécurité requis par le bénéficiaire.

Le titulaire est informé 15 jours à l'avance (date de l'audit, modalités financières pour le bénéficiaire et le titulaire, etc.).

Le bénéficiaire, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

6.11. Acquisition, développement et maintenance des systèmes d'information

6.11.1. Exigences de sécurité applicables aux systèmes d'information

Les exigences liées à la sécurité de l'information (exigences légales et réglementaires, objectifs et niveau de sécurité attendu) doivent être intégrées aux exigences des systèmes d'information tout au long de leur cycle de vie.

6.11.2. Sécurité des processus de développement et d'assistance technique

Pour un développement, le titulaire devra, à la livraison des composants applicatifs, s'assurer que le niveau de sécurité atteint est conforme aux exigences du bénéficiaire.

Le titulaire s'engage à mettre en œuvre :

- Une procédure de gestion des versions applicatives.
- Des mécanismes de verrouillage des sessions applicatives et de déconnexion automatique.

Le titulaire s'engage à sécuriser les accès du code source et des éléments associés (spécifications fonctionnelles, détaillées...).

Des bonnes pratiques (par exemple, OWASP) sont mis en place par le titulaire pour le développement sécurisé d'applications internet et intranet.

A chaque fin de développement, le titulaire s'engage à réaliser une phase de test et de recette de sécurité permettant de vérifier la bonne mise en œuvre des mesures de sécurité couvrant les vulnérabilités majeures (OWASP, MITRE, ...).

Le titulaire s'engage à transmettre au bénéficiaire le plan de recette de sécurité et les résultats des tests de sécurité.

Des tests d'intrusion sont réalisés au minimum annuellement pour les applications accessibles sur internet. Ces tests sont planifiés conformément à un calendrier annuel prédéfini ciblant des campagnes par produit et par périmètre fonctionnel.

Les recettes sécurité et les tests d'intrusion doivent être obligatoirement accompagnés d'un plan de corrections et d'un suivi de ce dernier.

6.11.3. Données de test

Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.

Les données de production (notamment les données à caractère personnel) ne peuvent pas servir de données de test à moins d'avoir été anonymisées auparavant.

6.12. Gestion des incidents liés à la sécurité de l'information

Le titulaire doit mettre en place un processus de gestion des incidents intégrant :

- La mise en place de procédures formelles de remontée d'information et de signalement des événements et incidents liées à la sécurité de l'information.
- Le signalement, le plus rapidement possible, de tout événement ou incident de sécurité au bénéficiaire.
- La sensibilisation de tous les intervenants aux procédures de signalement des différents types d'événements et d'incidents de sécurité susceptibles d'avoir une incidence sur la sécurité des données du bénéficiaire.

Le titulaire s'engage à détecter et à consolider les événements de sécurité associés aux accès logiques sur les environnements utilisés par le bénéficiaire.

Le titulaire tiendra informé le bénéficiaire du type d'investigation en cours et des Vulnérabilités ou risques que cet Incident de Sécurité aurait révélés concernant les services rendus au

bénéficiaire.

Dans le cadre de la détection des Incidents de sécurité, le titulaire s'engage à détecter tout Incident de Sécurité physique, organisationnel et logique, d'en alerter le bénéficiaire et de mener les actions permettant dans les meilleurs délais de couvrir les risques détectés en tenant informé le bénéficiaire.

Le titulaire s'engage sur sa capacité à réagir efficacement aux Incidents de sécurité détectés et à les résoudre de manière rapide, formelle et efficace afin d'en limiter les impacts pour le bénéficiaire.

6.13. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.

6.14. Cas de service hébergé en dehors du SI du bénéficiaire et de prestation de type Cloud Saas/laas et infogérance dans le SI du bénéficiaire

1. Les services hébergés devront respecter les exigences de sécurité des réglementations en vigueur.
2. Dans le cas des données de santé, en aucun cas l'hébergement pourra se faire hors Union Européenne.
3. Si des données de santé sont « hébergées » (cf sens donné par le Code de la Santé Publique) chez le titulaire ou un de ses sous-traitants celui-ci doit être certifié hébergeur de données de santé conformément à l'article L 1111-8 du Code de la Santé Publique.
4. Si des données à caractère personnel font l'objet de traitement par le système, le titulaire devra, à tout moment, respecter les exigences du RGPD et de la Loi Informatique et Libertés.
5. Pour s'assurer du respect de ces exigences, à tout moment le bénéficiaire est autorisé par le titulaire à commander un audit tel que décrit au paragraphe « Conformité ».

6.14.1. Accès par des utilisateurs du bénéficiaire au service hébergé

6. Une authentification d'accès doit permettre aux utilisateurs d'accéder aux services avec un niveau de sécurité adapté aux données à protéger. Les utilisateurs pourront changer leur authentifiant (mot de passe ou moyen d'authentification). La confidentialité des mots de passe doit être garantie par l'hébergeur lors de son stockage (chiffré) et de sa saisie.
7. Pour l'accès aux données de santé l'authentification devra être conforme aux exigences d'authentification forte de l'Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé.
8. Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données. Le chiffrement utilisé doit être conforme au RGS.
9. Le titulaire doit remettre un compte et authentifiant pour audit à la demande du

bénéficiaire et accepte que le bénéficiaire réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.

6.14.2. Continuité du service hébergé

10. Le service ne doit pas être indisponible plus que la durée décrite dans le CCTP.

6.14.3. Réversibilité du service hébergé

11. Une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits) est transmise au bénéficiaire 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration.
12. Une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits) est transmise au bénéficiaire en fin de contrat.

6.14.4. Garantie de Confidentialité des données hébergées

13. Le titulaire s'engage à garantir un accès aux données aux seules personnes habilitées selon les besoins du bénéficiaire
14. Les intervenants sont identifiés et doivent signer un engagement de confidentialité individuel. Les accès et actions réalisées devront être tracés.
15. Le titulaire s'engage à détruire les données selon les dispositions prévues dans le CCTP ou à défaut en fin de contrat après les avoir restituées au bénéficiaire sous une forme exploitable. Pour prouver la réalisation de cette destruction le titulaire s'engage à fournir un procès-verbal au bénéficiaire.

6.14.5. Solution est installée dans l'infrastructure informatique du bénéficiaire mais administrée intégralement par le titulaire

16. Le titulaire doit s'engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant prioritairement les dispositifs de lutte contre les codes malveillants avec au minimum un antivirus et EDR.
17. Le système d'exploitation ainsi que tous les composants seront mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire.
18. L'accès depuis l'extérieur du SI du titulaire pour l'exploitation et la maintenance doivent respecter les conditions décrites au paragraphe « Infrastructures et télémaintenance »
19. Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit à la demande du bénéficiaire et accepte que le bénéficiaire réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.
20. Les échanges avec l'extérieur du SI du bénéficiaire doivent être sécurisés : utilisation de protocoles sécurisés, du filtrage et du contrôle par les équipements de sécurité du bénéficiaire (le bénéficiaire se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure).

6.14.6. Perte ou le renouvellement de certification d'hébergement de données de santé

21. Le titulaire certifié hébergeur de données de santé doit transmettre au bénéficiaire, dans les 10 jours, les résultats des audits de certification, de contrôle et de renouvellement.