

Document à valeur institutionnelle

Exigences SSI simplifiées à destination des fournisseurs

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

Sommaire

1. Objet	2
2. Domaine d'application	2
3. Référence(s) et document(s) annexe(s).....	2
3.1. Référence(s)	2
3.1.1. Références documents internes.....	2
3.1.2. Références externes.....	2
3.2. Document(s) annexe(s)	2
5.1. Responsabilités.....	3
5.2. Personnes ressources.....	3
6.1. Organisation de la sécurité de l'information.....	4
6.2. La sécurité des ressources humaines.....	4
6.3. Gestion des actifs	4
6.4. Contrôle d'accès	5
6.5. Cryptographie	5
6.6. Sécurité physique et environnementale	5
6.7. Sécurité liée à l'exploitation.....	5
6.8. Sécurité des communications	6
6.9. Conformité	6
6.10. Acquisition, développement et maintenance des systèmes d'information	6
6.11. Gestion des incidents liés à la sécurité de l'information.....	7
6.12. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	7

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 n'y a pas d'interconnexion avec le système d'information du GHT Sud Lorraine ou dans le cas où le titulaire n'accède pas, ne traite pas, ne stocke pas, ne manipule pas des données sensibles ou ne fournit pas des composants d'infrastructure informatique.

2. Domaine d'application

Les exigences 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

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 patches 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.

6.1. 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 ...).

6.2. 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.

6.3. Gestion des actifs

Le titulaire dispose et tient à jour un inventaire des actifs informatiques où sont traitées les données du bénéficiaire. En cas d'échéance ou de résiliation du Contrat, le titulaire permet au bénéficiaire de récupérer une copie de l'intégralité des données dans un format exploitable par le bénéficiaire, puis dans un second temps à détruire toutes les copies des Données détenues dans ses systèmes informatiques.

Le titulaire protège la confidentialité des données sur les médias amovibles et lors des transferts à des tiers autorisés. 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 du marché et plus particulièrement pour les matériels de stockage, aucune donnée ne doit rester sur celui-ci qui pourrait entraîner la divulgation d'informations du bénéficiaire.

6.4. Contrôle d'accès

Le titulaire établit une politique de contrôle d'accès sur la base des enjeux de sécurité et en définissant des profils d'habilitations.

Il met en place des procédures formelles pour contrôler les droits d'accès aux systèmes et services d'information du titulaire (hébergeant les données du bénéficiaire) couvrant tout le cycle de vie de l'accès utilisateur, incluant une revue au minimum annuelle des droits et des comptes d'accès.

Le Prestataire met en œuvre :

- Les moyens nécessaires pour garantir l'unicité des identités des utilisateurs
- Une politique de mot de passe utilisateur conforme aux recommandations de l'ANSSI
- Une limitation du nombre de tentatives d'accès présentant un authentifiant erroné

Le titulaire met en œuvre un dispositif de séparation garantissant l'étanchéité des environnements utilisateurs et des données dans les environnements support et sous toutes leurs formes (stockage, mémoire, transmission, ...). Le titulaire différencie l'interface d'administration de l'interface permettant l'accès des utilisateurs finaux.

6.5. Cryptographie

Le titulaire met en œuvre des méthodes de chiffrement basés sur des standards publics éprouvés, à l'état de l'art, permettant à toute donnée du bénéficiaire d'être notamment transmise de façon sécurisée.

6.6. Sécurité physique et environnementale

Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant l'information sensible. Le titulaire applique des mesures de sécurité physique aux bureaux, aux salles et aux équipements, en particulier pour se protéger des désastres naturels, d'attaques malveillantes ou d'accidents.

6.7. Sécurité liée à l'exploitation

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

Le titulaire met en œuvre des systèmes de détection pour faciliter la détection rapide, l'investigation et la résolution des incidents de sécurité ; notamment des solutions de lutte contre les codes malveillants.

Le titulaire installe les correctifs logiciels le plus tôt possible sur ses applications et ses systèmes. Une politique de sauvegarde des données est définie précisant la fréquence et durée de rétention. Les sauvegardes des données stockées sur les moyens du titulaire sont sous sa responsabilité. Le titulaire mène des tests de restauration réguliers. Les données sauvegardées à l'extérieur sont au préalable chiffrées.

6.8. Sécurité des communications

Le titulaire limite les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Le titulaire limite les accès Internet en bloquant les services non nécessaires.

Les réseaux Wi-Fi utilisent un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK) et les réseaux ouverts aux invités sont séparés du réseau interne.

Le titulaire impose un VPN pour l'accès à distance et s'assure qu'aucune interface d'administration n'est accessible directement depuis Internet.

Le Prestataire met en œuvre la version la plus récente du protocole TLS sur tous les sites web et rend son utilisation obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.

Les pièces sensibles transmises via la messagerie électronique sont chiffrées et la clé de chiffrement est transmise via un canal distinct (par exemple par SMS).

6.9. Conformité

Le titulaire a mis en place et maintient un plan et processus de contrôle en matière de sécurité de l'information.

A la demande du bénéficiaire, le titulaire fournira un rapport d'évaluation (test d'intrusion, audit sécurité...) et le plan d'action associé.

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

Les exigences liées à la sécurité des systèmes d'information doivent être intégrées aux exigences des nouveaux développements et à la maintenance des systèmes existants.

Le titulaire met en place des frameworks et bonnes pratiques (par exemple, OWASP) pour le développement sécurisé d'applications internet et intranet. Le titulaire s'engage à réaliser une phase de test et de recette de sécurité couvrant les vulnérabilités majeures (OWASP, MITRE, ...).

Le titulaire met en œuvre sur les services des mécanismes de verrouillage des sessions applicatives et de déconnexion automatique.

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.

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

Le titulaire s'impose la mise en place d'un processus de gestion des incidents incluant :

- Des procédures de signalement des événements et incidents de sécurité auprès du bénéficiaire
- La sensibilisation de ses intervenants à ces procédures

Le titulaire s'engage à notifier le bénéficiaire de toute violation de la confidentialité des données à caractère personnel sous 24 heures dès sa détection.

Il garde un journal avec la description de l'incident et des données compromises (si connues), les coordonnées du déclarant et de la personne à qui l'incident a été communiqué, les mesures prises pour le résoudre (personnes en charge, et les données qui ont pu être récupérées), les éventuelles conséquences (pertes, divulgation, altération) qui en ont résulté.

6.12. 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