**SOMMAIRE**

[1 Introduction 2](#_Toc63321881)

[2 Exigences GENERALES sur les logiciels 3](#_Toc63321882)

[3 Identités 6](#_Toc63321883)

[4 Authentification et Single Sign On 7](#_Toc63321884)

[5 GESTION DES HABILITATIONS 9](#_Toc63321885)

[6 Tracabilité 10](#_Toc63321886)

[7 Protection des systèmes 12](#_Toc63321887)

[8 CRYPTOGRAPHIE 13](#_Toc63321888)

[9 MAINTENANCE ET TELEMAINTENANCE 14](#_Toc63321889)

[10 Specifications wi-fi 19](#_Toc63321890)

[11 Protection des donnees medicales 20](#_Toc63321891)

[12 CAS PARTICULIERS SELON PERIMETRE 21](#_Toc63321892)

[13 Glossaire des termes employés 26](#_Toc63321893)

# Introduction

Les solutions informatiques déployées au sein du Système d’Information du CHR METZ-THIONVILLE doivent :

* Satisfaire les exigences de sécurité informatique définies dans la politique cadre de sécurité du CHR METZ-THIONVILLE.
* Respecter les préconisations en matière de sécurité de l’ANS, l’ANSSI et du Ministère de la santé (PSSI –MCAS qui pourra être fournie sur demande).
* Respecter les préconisations en matière de protection des données dans le cadre du RGPD
* Respecter les exigences complémentaires propres à des systèmes critiques spécifiques

Les **exigences de sécurité sont obligatoires** leur non-respect est éliminatoire et elles sont notées **O comme Obligatoire (en début d’exigence) dans ce document.**

Les **recommandations sont des orientations techniques** fortement souhaitées en matière de sécurité pour apporter une cohérence avec les bonnes pratiques et recommandations du secteur santé. Elles sont notées **R comme Recommandé**.

Toutes les cases « description de la prise en charge » doivent être renseignées. Si une règle n’est pas applicable la mention N/A est inscrite et doit être justifiée.

Elles seront prises en compte dans l’évaluation technique de l’offre.

# Exigences GENERALES sur les logiciels

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 2.1 | **O** | Le titulaire s’engage à fournir la liste exhaustive des logiciels installés, documentée (niveau de version, prérequis, …) et contenant les informations détaillant chaque logiciel ainsi que les interactions entre eux. |  |  |
| *2.2* | ***O*** | Pour tout ce qui est fourni au titre de l’offre, le titulaire s’engage à acquérir et à concéder au CHR METZ-THIONVILLE l’ensemble des licences d’utilisation nécessaires à son bon fonctionnement.  Si nécessaire il détaillera les conditions spécifiques ou exclusions.  Ceci concerne l’ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance, …). |  |  |
| 2.3 | **O** | Le titulaire s’engage à n’installer et n’activer que les seuls logiciels nécessaires au bon fonctionnement de sa solution et de ce qui est attendu par le CHR METZ-THIONVILLE. |  |  |
| 2.4 | **O** | Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul. Ils devront aussi respecter les exigences de sécurité. |  |  |
| 2.5 | **O** | Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité. |  |  |
| 2.6 | **O** | Pour les logiciels de type SaaS (Software as a Service : logiciel hébergé), la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité. |  |  |
| 2.7 | **O** | Les personnels du titulaire devront respecter la charte d’accès et d’utilisation du Système d’Information du CHR METZ-THIONVILLE lors de toute intervention à l’installation ou en maintenance. Le titulaire s’engage à en informer ses personnels. |  |  |
| 2.8 | **O** | Toute opération réalisée par le titulaire et ses personnels lors de l’installation devra respecter les mêmes règles que celles décrites dans le chapitre Maintenance et Télémaintenance durant son exécution. |  |  |
| 2.9 | **R** | Les logiciels types *Auto-logon* ne sont pas souhaités hors cas particulier à décrire. |  |  |
| 2.10 | **R** | Lorsque des données à caractère personnel sont gérées par l’application, le titulaire fournit une procédure ou un outil d’anonymisation pour pouvoir être appliqué à tout autre environnement que celui de production. |  |  |
| 2.11 | **R** | Les applications ou services nécessitant un fonctionnement permanent, doivent être hébergés sur des machines ayant un système d’exploitation de type serveur et ne doivent pas dépendre d’une session utilisateur (fonctionnement en mode service). |  |  |
| 2.12 | **R** | Seules des versions de système d’exploitation maintenues par l’éditeur en termes de mise à jour de sécurité doivent être installées.  Le titulaire décrira tous les cas particuliers nécessitant une protection supplémentaire. |  |  |
| 2.13 | **O** | Si la solution proposée doit être hébergée sur un serveur du CHR METZ-THIONVILLE, elle doit être compatibles avec les prérequis fournis par la DSI. |  |  |
| 2.14 | **R** | Si la solution proposée comporte des objets connectés (IOT), un rapport d’audit par un organisme spécialisé indépendant du titulaire est demandé avec la réponse. |  |  |
| 2.15 | **O** | Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d’application et accepter des audits de vérification de conformité. Les clauses spécifiques au RGPD fournies en annexe dédiée doivent être signées par le représentant légal du sous-traitant. |  |  |

# Identités

Le CHR METZ-THIONVILLE a pris le parti d’établir le service d’annuaire de la société Microsoft (AD : Active Directory) en référentiel garant de l’unicité des comptes utilisateurs.

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 3.1 | **O** | L’exploitation de cet annuaire comme source d’identité logicielle est fortement souhaitée et peut revêtir deux formes :   * Déport de la gestion d’identité de l’application au sein de l’annuaire du CHR METZ-THIONVILLE. * Mise à disposition d’un point d’entrée (web service, connecteur…) permettant au CHR METZ-THIONVILLE de synchroniser le référentiel d'identités de l’application avec son référentiel d’identité et d’authentification (IAM).   En l’absence de ces modes le titulaire décrira la gestion des identités au sein de son dispositif. |  |  |
| 3.2 | **R** | Cas de systèmes (biomédicaux par exemple) installés sur un poste de travail du CHR METZ-THIONVILLE avec besoin de comptes locaux ou de systèmes autonomes pour gérer les comptes au sein du logiciel : le titulaire décrira au moins le mode permettant d’installer le logiciel sur un répertoire partagé fourni par la DSI dont la sécurité d’accès est prise en charge par un groupe de sécurité et l’annuaire. |  |  |

# Authentification et Single Sign On

Le CHR METZ-THIONVILLE n’envisage l’authentification unique (Single Sign On) qu’au travers de l’identité de domaine portée par les protocoles communément utilisés en environnement Windows.

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 4.1 | **O** | Les mots de passe des comptes nécessaires à l’administration de la solution doivent pouvoir être modifiés par le CHR METZ-THIONVILLE. |  |  |
| 4.2 | **R** | S’agissant des applications WEB, l’usage des protocoles NTLM notamment SSO ou Kerberos notamment mot de passe crypté est attendu en vue de perpétuer implicitement et de manière sécurisée l’identité de l’utilisateur connecté au serveur web. |  |  |
| 4.3 | **R** | Concernant les applications usant d’un client lourd :   * Lorsque le référentiel d’identités de l’application est déporté dans l’AD, l’authentification auprès d’un serveur AD du ticket de session associé au processus applicatif est fortement préconisée. Si l’application n’offre pas – en l’état – la possibilité de récupérer l’identité Windows, un plan d’intégration le permettant est souhaité. A minima, l’authentification de l’utilisateur par mot de passe reposera sur LDAP. * Lorsque le référentiel d’identités est propre à l’application et seulement synchronisé à l’AD, la simple récupération de l’identité du propriétaire du processus applicatif pourra être tolérée dans l’attente d’une intégration de LDAP à l’application. Ce mode transitoire aux bonnes pratiques est justifié lors du recours à une authentification forte (CPS ou équivalent) à l’ouverture de session Windows. |  |  |
| 4.4 | **R** | Dans le cas d’architecture N-Tiers, l’origine de la connexion fera partie du processus d’authentification. Ainsi lorsque l’application permet la propagation des identités utilisateurs jusqu’aux données, l’utilisateur ne saurait se connecter directement au SGBD. La chaine d’accès devra donc être garantie pour chaque strate applicative. |  |  |
| 4.5 | **O** | Pour les applications web exposées sur internet et qui intègreraient une authentification et/ou une gestion des comptes :  Les pages réservées à l’authentification et à la création de comptes doivent intégrer un dispositif de prémunition contre l’usage de robots.  Des mécanismes empêchant de réutiliser des informations de connexion ou de session pour contourner l’authentification doivent être en place. |  |  |
| 4.6 | **O** | Pour les applications web exposées sur internet et qui intègreraient une authentification et/ou une gestion des comptes, les mécanismes d’authentification doivent être adaptés à la criticité des données.  Une authentification forte est exigée pour l’accès à des données de santé par carte CPS ou équivalent (sauf disposition contraire qui conduirait le CHR METZ-THIONVILE à prendre en charge une authentification forte en préalable à l’accès à l’application : cas d’un portail d’authentification en amont de l’application). |  |  |
| 4.7 | **R** | Pour les applications web un audit externe de sécurité de type top 10 de l’OWASP sera fourni avec l’offre. |  |  |

# GESTION DES HABILITATIONS

| **Ref.** |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| **5.1** | **R** | La gestion des habilitations doit reposer sur le moteur d’habilitation du CHR METZ-THIONVILLE, (Hpliance). Ce moteur fournit pour chaque utilisateur un ensemble d’information dont notamment le profil à utiliser dans l’application (fonctionnalités autorisées) et son périmètre d’habilitation (liste des Unités Fonctionnelles pour lesquelles il peut accéder aux informations).  L’accès à l’Hpliance peut se faire de diverses façons :   * Appel de web service * Provisionning par EAI * Dans la mesure où seule la notion de profil (telle que mentionnée ci-dessus, indépendante donc de l’affectation sur des Unité d’affectation de la personne) serait nécessaire, l’utilisation de groupe AD est envisageable. * Intégration spécifique, auquel cas l’éditeur devra fournir les éléments pour un accès direct et documenté à son système d’habilitation ne présentant pas de risque pour le fonctionnement du produit (web service, tables de base de données, procédures stockées …) |  |  |

# Tracabilité

Les exigences fonctionnelles de traçabilité peuvent être supérieures à celle citées ici d’une manière générale pour la sécurité.

Le CHR METZ-THIONVILLE met en œuvre la centralisation de ses traces applicatives et systèmes au sein d’un dispositif unique afin d’en garantir l’intégrité, la conservation et la bonne exploitation et protection ;

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 6.1 | **O** | Les traces produites devront être accessibles par l’outil de centralisation des traces du CHR METZ-THIONVILLE dans un format et un mode d’accès rendus possibles et décrits par le titulaire (ATNA : format IHE, Syslog, requête dans une base de données à fournir, fichier à décrire). |  |  |
| 6.2 | **R** | La solution proposée doit exposer de manière sécurisée ses éléments de traçabilité. Décrire les systèmes d’accès. |  |  |

Contenu de la trace :

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 6.3 | **O** | Les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec. |  |  |
| 6.4 | **O** | La capacité (ou non) à tracer toutes les actions (y compris la consultation de données) doit être décrite. |  |  |
| 6.5 | **R** | Les traces produites devront être accessibles par l’outil de centralisation des traces du CHR METZ-THIONVILLE dans un format et un mode d’accès rendus possibles et décrits par le titulaire (ATNA : format IHE, Syslog, requête dans une base de données à fournir, fichier à décrire). |  |  |
| 6.6 | **R** | S’agissant des modifications de valeurs sensibles au sein du dispositif, il est souhaité que les traces correspondantes comportent la valeur en amont et en aval de l’événement. La suppression d’une donnée du point de vue applicatif ne saurait engendrer la perte de l’historique des accès et modifications associées à cette donnée. |  |  |
| 6.7 | **R** | Lorsque la gestion des autorisations applicatives – même partiellement – est du ressort de l’application, il est souhaitable que tout événement relatif à l’édition d’un profil ou d’un utilisateur soit tracé. |  |  |
| 6.8 | **R** | Dans le cas d’architectures N-Tiers ou lors de l’usage de comptes applicatifs, les traces devront comporter l’utilisateur d’origine et l’ordinateur source de la connexion. Si cela s’avérait impossible, la mise en corrélation des traces des différentes strates applicatives par le biais des identifiants de session devra permettre de déterminer avec certitude la continuité de l’accès. |  |  |

# Protection des systèmes

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 7.1 | **O** | Le titulaire s’engage à mettre en œuvre les dispositifs et paramétrages nécessaires pour prémunir ses systèmes contre les attaques virales et intrusives selon l’une des formes suivantes :   * Intégration de ses dispositifs dans la démarche sécurité du CHR METZ-THIONVILLE en installant l’antivirus du CHR METZ-THIONVILLE et en inscrivant ses systèmes dans les règles de gestion des correctifs de sécurité en vigueur pour le reste du SI. * Déploiement de ses propres utilitaires et politiques de mise à jour si l’intégration des dispositifs du CHR METZ-THIONVILLE ne sont pas réalisables techniquement. * Les types de fichiers nécessitant une exclusion d’analyse par l’antivirus conditionnant le bon fonctionnement doivent être communiqués pour décider d’un éventuel complément de sécurité * A défaut, ou en cas d’une insuffisance de l’analyse antivirale, une solution de sécurité externe en interface avec la solution sera installée (équipement de type pare-feu avec antivirus).   De fait, en cas d’intrusion ou de contamination, le titulaire est responsable de la vulnérabilité de ses systèmes vis à vis des définitions virales et correctifs publics. |  |  |

# CRYPTOGRAPHIE

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 8.1 | **O** | Dans le cas d’applications web publiées sur internet comme sur l’intranet, l’usage de TLS est impératif. Le titulaire pourra recourir à des certificats fournis par le CHR METZ-THIONVILLE. |  |  |
| 8.2 | **O** | Les données utiles à l’authentification doivent être chiffrées lors de leur communication et de leur stockage. |  |  |
| 8.3 | **O** | De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux standards du marché, et au Référentiel Général de Sécurité (RGS). |  |  |

# MAINTENANCE ET TELEMAINTENANCE

Lorsqu’une télémaintenance est prévue par le titulaire, des règles strictes doivent être prises en compte :

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 9.1 | **O** | Pour ce qui concerne la remontée d’informations issues des dispositifs maintenus vers votre site de diagnostic, cet envoi doit être décrit précisément en indiquant toutes les données transférées. Cet usage exclusif à des fins de surveillance du maintien en condition opérationnelle et l’absence de données personnelles directement ou indirectement liées à nos patients doit être garanti.  Cette remontée d’information devra utiliser des protocoles sécurisés, être tracée et passer par nos passerelles de contrôle d’accès à internet ou par un VPN IPSEC site à site avec votre site de télédiagnostic (recommandé). |  |  |
| 9.2 | **O** | La connexion de télémaintenance doit se faire via la passerelle Internet sécurisée mise à disposition par le CHR METZ-THIONVILLE (VPN IPSEC ou VPN SSL). La demande de ce VPN devra suivre la procédure du CHR METZ-THIONVILLE. |  |  |
| 9.3 | **O** | Au niveau des postes de travail standard du CHR METZ-THIONVILLE, aucun outil de prise de contrôle à distance ne peut être installé dans le cadre d’une application. Le seul outil de prise à contrôle à distance autorisé est celui servant à l’administration système gérée par la DSI du CHR METZ-THIONVILLE. |  |  |
| 9.4 | **O** | Il est de la responsabilité du titulaire d’assurer la sécurité de sa plateforme d’intervention à distance (données et logiciels) |  |  |
| 9.5 | **O** | Le CHR METZ-THIONVILLE se réserve le droit de faire (ou de faire faire) des contrôles de sécurité de façon périodique ou ponctuelle chez le titulaire afin de s’assurer que le niveau de sécurité requis est conforme aux exigences de sécurité en vigueur. |  |  |
| 9.6 | **O** | Le titulaire doit avoir une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance. |  |  |
| 9.7 | **R** | Les postes de télémaintenance doivent être isolés physiquement du réseau local du titulaire. |  |  |
| 9.8 | **O** | Les données à caractère personnel ou technique du CHR METZ-THIONVILLE (configuration des équipements) exploitées par les équipes de support chez le titulaire ne doivent pas être divulguées (une protection adaptée doit être réalisée). |  |  |
| 9.9 | **O** | L’intervention de maintenance est encadrée par un règlement, un contrat ou une convention entre le CHR METZ-THIONVILLE et le titulaire, définissant les engagements de chacun, les modalités pratiques, … |  |  |
| 9.10 | **O** | Le titulaire s’engage sur la sécurité de la prestation, son représentant légal devra signer l’engagement titulaire de maintenance fourni par la DSI rappelant la confidentialité des données et l’engageant à informer ses personnels que tous les accès et actions seront tracés. |  |  |
| 9.11 | **O** | Il est de la responsabilité du titulaire de restreindre les accès physiques et logiques de ses postes aux seules personnes autorisées (par sensibilisation et mise à disposition de moyens de sécurité adéquats). |  |  |
| 9.12 | **O** | Il est de la responsabilité du titulaire de connaitre en toutes circonstances l’identité de toute personne qui se connecte ou s’est connectée sur la plateforme de télémaintenance et d’en assurer la traçabilité (cette traçabilité pourra être communiquée sur demande du CHR METZ-THIONVILLE). |  |  |
| 9.13 | **O** | Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l’issue d’une intervention soient supprimées. |  |  |
| 9.14 | **O** | Le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs connectés et met à disposition les correctifs et préventifs nécessaires dans les délais appropriés. |  |  |
| 9.15 | **O** | Le titulaire s’engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du titulaire, la correction et la prise en charge des impacts à sa charge. |  |  |
| 9.16 | **R** | Le titulaire garantit la mise à niveau de ses logiciels et plateformes en cas d’obsolescence du système d’exploitation.  Il en est de même pour tous les autres logiciels indispensables au bon fonctionnement du dispositif.  A défaut il fournira à titre gracieux les moyens pour maintenir un niveau de sécurité suffisant. |  |  |
| 9.17 | **O** | Le titulaire doit fournir un rapport détaillé de l’intervention effectuée, un modèle pourra être fourni. |  |  |
| 9.18 | **O** | Si le CHR METZ-THIONVILLE dispose d’un bastion d’administration ou le met en place ultérieurement le titulaire s’engage à l’utiliser pour accéder aux systèmes qu’il devra maintenir ou exploiter (de fait l’accès direct aux serveurs et applications est interdit).  Selon les besoins d’intervention l’accès aux systèmes à maintenir ou exploiter sera ouvert et fermé par la DSI à la demande (du mainteneur ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance).  Si l’établissement ne dispose pas d’un bastion d’administration, le cas d’utilisation d’un bastion équivalent du titulaire pourra être étudié s’il apporte les mêmes garanties de protection, de traçabilité, de preuve opposable et d’accès avec la possibilité d’audit (une description précise devra être fournie). |  |  |
| 9.19 | **R** | Le titulaire pourra établir un PAS (Plan Assurance Sécurité) afin de faire connaitre les dispositions de sécurité qu’il met en place pour sa prestation. Le PAS traite :   * Des critères de sécurités utilisés dans la désignation des personnes chargées des interventions. * De la désignation des sites d’exécution de la prestation, protection et accès physiques des locaux utilisés. * Des règles de protections des informations du Système d’Information associées à la prestation de télémaintenance. * De l’architecture générale de la plateforme d’intervention (cloisonnement technique etc.). * Des accès logiques à la plateforme, identification et authentification, mise en veille, déconnexion automatique, gestion des droits, traçabilité… * Des dispositions prises pour assurer la continuité de l’activité après un sinistre ou un incident majeur. * De l’assurance et des contrôles de la sécurité des services de l’intervention fournis. |  |  |

# Specifications wi-fi

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 10.1 | **O** | Le chiffrement et l’intégrité des informations circulant sur le réseau doivent être assurés par la mise en place sur les équipements concernés du mécanisme WPA2 ou ultérieurs garantissant le plus haut niveau de sécurité (version de la norme IEEE 802.11i certifiée par la Wifi Alliance). |  |  |
| 10.2 | **R** | Pour l’authentification l’association de WPA2 ou supérieur (« WPA2 – Entreprise ») avec un serveur d'authentification 802.1X (Radius) par le biais du protocole EAP est demandée. Pour éviter la gestion redondante des comptes, le serveur devra s’appuyer sur l’annuaire LDAP centralisé de l’établissement. Pour des équipements spécifiques qui seraient incompatibles avec ce paramétrage, une description des niveaux possibles et des compléments de sécurisation doivent être fournis pour évaluation d’un mode de prise en charge de la sécurité acceptable. |  |  |

# Protection des donnees medicales

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 11.1 | **O** | Le titulaire et son personnel, le personnel du CHR METZ-THIONVILLE sont soumis à un engagement de confidentialité conformément aux préconisations de la CNIL, du RGPD et au Code de la Santé Publique. Ces articles s’adressent notamment aux titulaires extérieurs. |  |  |

**Article L1110-4 du Code de la Santé Publique**

*….Excepté dans les cas de dérogation expressément prévus par la loi, ce secret (secret médical) couvre l’ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes.* ***Il s’impose à tout professionnel de santé ainsi qu’à tous les professionnels intervenant dans le système de santé****.*

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 11.2 | **O** | En conséquence, notamment, les jeux de données fournies par le CHR METZ-THIONVILLE sont strictement confidentiels et sont liés au secret professionnel. |  |  |
| 11.3 | **R** | Un outil de codage des données est souhaité. Cet outil doit permettre de banaliser les informations de la base de données ou bien des fichiers de données pour préserver le secret médical. |  |  |
| 11.4 | **R** | En outre, cet outil doit préserver l’anonymat des personnes si cela est le cas dans les données de tests. |  |  |

# CAS PARTICULIERS SELON PERIMETRE

* Cas de moyens mobiles :

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.1 | **O** | Tout dispositif mobile doit être chiffré (en conformité avec le Référentiel Général de Sécurité : RGS) et les clefs de chiffrement doivent être remises au CHR METZ-THIONVILLE. |  |  |

* Cas de service hébergé en dehors du Système d’information de la DSI (pour **tout ou partie)** et cas de services installés dans le SI du CHR METZ-THIONVILLE mais administrés en autonomie par le titulaire

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.2 | **O** | Si le centre de maintenance ou d’hébergement est en dehors du territoire national cela devra être précisé pour analyser les contraintes réglementaires associées au type de système à protéger selon la politique de sécurité de l’état et du ministère de rattachement.  Le candidat doit préciser les pays où sont réalisés les hébergements. Dans le cas d’hébergement hors communauté européenne les dispositions adaptées doivent être préalablement réalisées et validées par les autorités compétentes. |  |  |
| 12.3 | **O** | Si des données de santé sont hébergées chez le titulaire ou un de ses sous-traitants celui-ci doit être agréé hébergeur de données de santé par l’ANS (ou toute commission compétente désignée par la réglementation). |  |  |
| 12.4 | **O** | Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d’application et accepter des audits de vérification de conformité. A cette fin sont annexées au contrat *les clauses de conformité au RGPD.* |  |  |
| 12.5 | **O** | Si des données nominatives à caractère personnel font l’objet de traitement par le système, une conformité au RGPD est nécessaire et le titulaire devra démontrer le niveau de protection adapté à la criticité de ces données. Cette démonstration doit être intégrée dans les descriptions de la prise en charge des mesures concernées du présent document, en accord avec *les clauses de conformité au RGPD* annexées au contrat. |  |  |

* **Concernant l’accès au service hébergé par des utilisateurs du CHR METZ-THIONVILLE :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.6 | **R** | Un accès identifié, authentifié et habilité selon les conditions décrites dans les paragraphes précédents (Identité, Authentification, Gestion des habilitations) pour un logiciel installé dans le SI du CHR METZ-THIONVILLE est fortement souhaité, en cas d’impossibilité technique, un identifiant sera communiqué aux utilisateurs ou un mode de gestion permettra à un utilisateur identifié comme administrateur des comptes utilisateurs de gérer les utilisateurs. |  |  |
| 12.7 | **O** | 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. Pour l’accès aux données de santé l’authentification devra être conforme aux exigences d’authentification forte de la CNIL et de l’ANS (carte CPS ou équivalent). |  |  |
| 12.8 | **O** | Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données. |  |  |
| 12.9 | **O** | Le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHR METZ-THIONVILLE et accepte que le CHR METZ-THIONVILLE réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité. |  |  |

* **Concernant la continuité du service hébergé :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.10 | **O** | Le service ne doit pas être indisponible plus de x heures (à préciser) |  |  |
| 12.11 | **R** | Une copie exploitable des données (fichier informatique avec champs délimités et décrits) est transmise ou accessible tous les x jours (mode de mise à disposition à décrire par le fournisseur) |  |  |

* **concernant La réversibilité du service hébergé :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.12 | **O** | Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise au CHR METZ-THIONVILLE 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration (mode de mise à disposition à décrire par le fournisseur) |  |  |
| 12.13 | **O** | Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise au CHR METZ-THIONVILLE T en fin de contrat (mode de mise à disposition à décrire par le fournisseur) |  |  |

* **Concernant La garantie de Confidentialité des données hébergées :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.14 | **O** | Le titulaire s’engage à garantir un accès aux données aux seules personnes habilitées selon les besoins du CHR METZ-THIONVILLE |  |  |
| 12.15 | **O** | Les intervenants sont identifiés et doivent signer un engagement de confidentialité individuel. Les accès et actions réalisées pourront être tracés. |  |  |
| 12.16 | **O** | Le titulaire s’engage à détruire les données en fin de contrat après les avoir restituées au CHR METZ-THIONVILLE sous une forme exploitable. |  |  |

* **Règles supplémentaires si la solution est installée dans l’infrastructure informatique du CHR METZ-THIONVILLE mais administrée intégralement par le titulaire :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Visa** |
| --- | --- | --- | --- | --- |
| 12.17 | **O** | Le titulaire doit s’engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant au moins un antivirus mis à jour et un système d’exploitation ainsi que tous les composants mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire. |  |  |
| 12.18 | **O** | L’accès depuis l’extérieur du CHR METZ-THIONVILLE pour l’exploitation et la maintenance doivent respecter les conditions décrites au paragraphe Maintenance et Télémaintenance. |  |  |
| 12.19 | **O** | Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHR METZ-THIONVILLE et accepte que le CHR METZ-THIONVILLE réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité. |  |  |
| 12.20 | **O** | Les échanges avec l’extérieur du CHR METZ-THIONVILLE doivent être sécurisés : utilisation de protocoles sécurisés et filtrage et contrôle par les équipements de sécurité du CHR METZ-THIONVILLE (le CHR METZ-THIONVILLE se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure. |  |  |

# Glossaire des termes employés

AD (Active Directory) : Service d’annuaire de la société Microsoft

Application Web : Architecture applicative reposant sur la mise à disposition par HTTP de contenus HTML dynamiques

HTTP (Hypertext Transfer Protocol) : protocole de communication client/serveur reposant sur le principe de requête/réponse vis-à-vis de ressources identifiées par une adresse réticulaire

IAM (Identity and Authorization Manager) : Service de gestion et de synchronisation des identités et autorisations entre les différents composants du système d’information

Kerberos : Protocole d’authentification reposant sur un chiffrement symétrique

LDAP (Lightweight Directory Access Protocol) : protocole standard de communication avec un service d’annuaire

NTLM : Protocole d’authentification reposant sur un mécanisme de challenge

OWASP : Open Web Application Security Project

PKI (Public Key Infrastructure): Dispositif de gestion des clefs publiques. Permet l’édition des bi-clefs nécessaires au cryptage asymétrique.

RGPD : Règlement Général sur la Protection des Données.

SGBD : Dispositif de dépôt et d’indexation de données permettant l’adressage de grands volumes

SOAP : Protocole applicatif mis en œuvre dans le cadre de web services reposant sur l’échange de flux XML par le biais d’un serveur HTTP.

Web Service : Service applicatif exposé sous forme d’API selon le protocole SOAP.

XML (Extended Markup Language) : « langage de balisage extensible[[1]](https://fr.wikipedia.org/wiki/Extensible_Markup_Language#cite_note-2) » en français) est un métalangage informatique de balisage générique.