|  |  |  |
| --- | --- | --- |
| LOGO_CHRMT | Processus | Référence : PROC/00024 |
| **Conformité et prérequis techniques DSI**  *Diffusion limitée :*  *Personnels des directions : DSI, DTPBMESI et DAHL*  *Prestataire de la solution* | Version : 03 |
| Date de publication :  10/01/2023 |
| Date de prochaine révision :  10/01/2027 |

La mise à jour de ce document est garantie sur Intranet – Veillez régulièrement à l’actualisation de vos éditions papier.

Pour toute information sur ce document, merci de contacter les rédacteurs et/ou le service qualité.

# CYCLE DE VIE

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Rédacteur** | **Relecteur** | **Valideur** |
| Nom | **M. Cyril PIERRÉ**  Ingénieur Sécurité SI | **M. Albert CRUMBACH**  RSSI, DPO, Responsable Réseaux SI  **M. Thierry KELLER**  Responsable Infrastructure SI  **M. André STIEN**  Responsable Support Informatique  **M. Mickael CHOPLIN**  Adjoint Directeur DSI | **M. Laurent KARMUSIK**  Directeur DSI |

# OBJET

Prérequis techniques à respecter pour toute solution informatique utilisée dans l’établissement.

# DOMAINE D’APPLICATION

Ce document s’applique à tous les prestataires et intervenants mettant en œuvre une application ou un équipement informatisé pour le CHR METZ-THIONVILLE.

# DEFINITIONS / ABREVIATIONS

* **CHR** : Centre Hospitalier Régional de METZ-THIONVILLE
* **GHT**: Groupement Hospitalier de Territoire
* **DSI**: Direction du Système d’Information
* **SI**: Système d’Information

# DOCUMENTS ASSOCIES

* **PROC/00024** : Conformité et prérequis techniques DSI (présent document)
* **PROC/00026** : Plan d’Assurance Sécurité SI (PAS)
* **PROC/00028**: Clauses Contractuelles types RGPD Client – Prestataire
* **PROC/0649 :** Charte d’utilisation des technologies numériques pour le personnel externe au CHR METZ-THIONVILLE

# REFERENCES

* **PGSSI-S** : Politique Générale de Sécurité des Systèmes d’Information de Santé
* **RGPD**: Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
* **PSSI MCAS**:Politique de Sécurité des Systèmes d’Informations des Ministères Sociaux

# DEVELOPPEMENT

Table des matières

[1. Conformité à la Politique de Sécurité SI du CHR 2](#_Toc256000000)

[2. Conformité réglementaire 2](#_Toc256000001)

[3. Hébergement de données 3](#_Toc256000002)

[a. Hébergement externalisée de données 3](#_Toc256000003)

[b. Hébergement dans le Datacenter de l’établissement 3](#_Toc256000004)

[c. Hébergement sur un poste de travail 4](#_Toc256000005)

[4. Prérequis techniques 4](#_Toc256000006)

[a. Configuration type des postes de travail 5](#_Toc256000007)

[b. Système d'exploitation 5](#_Toc256000008)

[c. Domaine Active Directory 6](#_Toc256000009)

[d. Gestion de la configuration matérielle 6](#_Toc256000010)

[e. Accès aux équipements 6](#_Toc256000011)

[f. Comptes et authentification 6](#_Toc256000012)

[g. Antivirus et EDR 7](#_Toc256000013)

[h. Chiffrement des flux 7](#_Toc256000014)

[i. Traçabilité des données 7](#_Toc256000015)

[j. Disponibilité des données 7](#_Toc256000016)

[5. Documents à fournir et enregistrements 8](#_Toc256000017)

[a. L'installation 8](#_Toc256000018)

[b. Enregistrements 8](#_Toc256000019)

[• Incidents 8](#_Toc256000020)

[• Interventions distantes 8](#_Toc256000021)

[6. Signature et engagement 8](#_Toc256000022)

## Conformité à la Politique de Sécurité SI du CHR

Le prestataire doit prendre un engagement de conformité sur chacun des documents suivants :

1. **PROC/00024** : Conformité et prérequis techniques DSI (présent document)
2. **PROC/00026** : Plan d’Assurance Sécurité SI (PAS)
3. **PROC/00028**: Clauses Contractuelles types RGPD Client – Prestataire
4. **PROC/0649 :** Charte d’utilisation des technologies numériques pour le personnel externe (signé par chaque intervenant)

## Conformité réglementaire

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Le prestataire s’engage à être en conformité avec la Politique de Sécurité des Systèmes d’Informations des ministères sociaux (PSSI-MCAS) qui est opposable aux établissements de santé ainsi qu’à leurs prestataires et fournisseurs | Obligatoire |  |
| L’hébergeur devra impérativement être certifié HDS dans le cas où des données de santé ou des données personnelles sont hébergées en dehors de l’infrastructure du CHR. | Obligatoire |  |

## Hébergement de données

### Hébergement externalisée de données

Dans le cas où des données de santé ou des données personnelles sont hébergées en dehors de l’infrastructure du CHR :

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Les connexions et les échanges de données devront être chiffrées. Le prestataire précisera ses mécanismes de connexion en précisant les types de sécurisation retenus. Ceux-ci devront être agréés par la DSI de l’établissement. | Obligatoire |  |
| L’application sera utilisable via un navigateur. Le prestataire précisera ses prérequis concernant le navigateur et/ou celui du poste de travail. Il détaillera notamment les périphériques associés à l’utilisation du logiciel. | * Oui * Non |  |

### Hébergement dans le Datacenter de l’établissement

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Le prestataire utilisera l’infrastructure de virtualisation VMware vSphere de l’établissement.  La haute disponibilité sera permise par les mécanismes de PRA/PCA du Datacenter.  Le serveur sera intégré à l’Active Directory. | * Oui * Non |  |
| Dans le cas extrême ou la virtualisation n’est pas possible, le prestataire pourra proposer la mise en œuvre d’un serveur physique. Dans ce cas il se chargera d’installer et de configurer tous les équipements liés au serveur en étant accompagné d’un membre de l’équipe infrastructure de la DSI et il devra fournir les accès d’administration à la DSI et se mettre en conformité avec les exigences de sécurité en fonction du type d’application et de données hébergées (sauvegarde, haute disponibilité, équilibrage de charge, supervision…). Le serveur sera intégré à l’Active Directory. | * Oui * Non |  |
| Le prestataire précisera la version de base de données utilisées parmi PostgreSQL, Oracle et SQL Server.  Deux Bases de Données devront être opérationnelles :   * Une Base de production * Une Base de test-formation pour tester les nouvelles versions du logiciel et/ou permettre la formation des utilisateurs sans perturber la production des soins. | Obligatoire |  |
| L’ensemble des informations doit pouvoir être interrogé par une solution de Business Intelligence (QlikView, BO…), ce qui implique de connaître le schéma de structure de la base de données de la solution proposée et de mettre à disposition un connecteur permettant son interrogation.  Le prestataire devra :   * Soit mettre à disposition une base « DataWareHouse » interrogeable et documentée en précisant la périodicité de synchronisation avec la base de production * Soit permettre l’interrogation de la base de données de production (généralement les données de J-1 sont extraites toutes les 24h durant les périodes de moindres activités, par défaut en nuit profonde) | Obligatoire |  |
| Les applications proposées avec la solution seront de préférence déployées via les serveurs Citrix de l’établissement au lieu d’installations individuelles sur les postes de travail.  La solution est compatible Citrix et si possible dispose de l’agrément « Citrix Ready »  Il est impératif d’indiquer le nombre de session simultanée sur un même serveur Citrix à des fins d’optimisation. | * Oui * Non |  |

### Hébergement sur un poste de travail

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Si la solution n’est pas hébergée sur un serveur, le prestataire précisera dans le détail les prérequis en termes de configuration matérielle et logicielle du poste de travail qui devront être validées par la DSI de l’établissement avant déploiement. Un plan de sauvegarde devra être mis en place | Obligatoire |  |

## Prérequis techniques

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Seul le protocole TCP/IP doit être configuré. Tous les autres devront être désactivés où faire l'objet d'une étude spécifique. | Obligatoire |  |
| Les PC du CHR sont en DHCP. Les serveurs et les postes « prestataires » sont en IP fixes sur des Vlans. Les protocoles NetBios et Wins seront désactivés. | Obligatoire |  |
| Les livrables de la solution devront comporter un synoptique complet de l’architecture réseau et des équipements en place. Ce synoptique devra comporter à minima :   * Plan de nommage et d’adressage * Flux entre les équipements (protocoles, débits, ports TCP/IP) * Numéros de prises | Obligatoire |  |
| L’accès à internet se fait par l’intermédiaire d’un proxy HTTPS. Si des accès directs sont nécessaires, ils devront être demandés à la DSI avec les adresses IP source et destination, les protocoles utilisés et les débits estimatifs. | Obligatoire |  |
| Si nécessité d’utiliser le serveur de messagerie de l’établissement, l’accès se fera par le protocole sécurisé SMTPS. | * Oui * Non |  |
| Avant la mise en œuvre, le prestataire devra fournir la liste exhaustive des flux à autoriser (communication serveur-serveur, serveur-client, client-client) | Obligatoire |  |

### Configuration type des postes de travail

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Si le prestataire met en place des postes de travail, ils devront respecter la configuration minimale suivante :   * UC : processeur de dernière génération * RAM : 8Go * SSD : 256 Go * Écran : 22’’ sur PC fixe (HDMI ou DP) / 15’’ sur PC portable * Windows en version professionnelle * Office LTSC 2021 Standard 64 bits recommandée | Obligatoire |  |

### Système d'exploitation

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| *Poste de travail* | | |
| Les postes de travail devront être en Windows 11 ou Windows 10 (uniquement si Windows 11 n’est pas supporté). | Obligatoire |  |
| Les mises à jour Windows seront installées au fil de l’eau par la DSI. | Obligatoire |  |
| Les changements de version de Windows seront installés dans un délai de 6 mois après la parution de la nouvelle version (exemple passage de Windows 11 v21H2 vers 22H2).  L’éditeur devra fournir une version de l’application compatible de sa solution avec la nouvelle version de Windows | Obligatoire |  |
| *Serveurs Windows* | | |
| Les serveurs seront en Windows Server 2022 ou Windows Server 2019 | Obligatoire |  |
| Les mises à jour Windows seront installées au fil de l’eau par la DSI selon la périodicité suivante :   * Pour les failles critiques, le délai d'application des correctifs de sécurité doit être réalisé aussi vite que possible dès réception de l’alerte * Sur le périmètre exposé sur Internet (DMZ), le délai d'application des correctifs de sécurité doit être inférieur à 14 jours après publication * Sur le périmètre interne pour les serveurs, le délai d'application des correctifs de sécurité doit être inférieur à 60 jours après publication | Obligatoire |  |
| *Serveurs GNU/Linux* | | |
| La distribution Linux installée doit avoir un cycle de vie d’au moins 3 ans à partir de la mise en œuvre de la solution. | Obligatoire |  |
| Les mises à jour seront installées au fil de l’eau par la DSI selon la périodicité suivante :   * Pour les failles critiques, le délai d'application des correctifs de sécurité doit être réalisé aussi vite que possible dès réception de l’alerte * Sur le périmètre exposé sur Internet (DMZ), le délai d'application des correctifs de sécurité doit être inférieur à 14 jours après publication * Sur le périmètre interne pour les serveurs, le délai d'application des correctifs de sécurité doit être inférieur à 60 jours après publication | Obligatoire |  |

**Les systèmes d'exploitation "Apple" ne sont pas pris en charge sauf demande explicite de l’établissement.**

### Domaine Active Directory

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Les postes et serveurs seront intégrés au domaine Active Directory de l’établissement.  Dans le cas contraire le prestataire devra motiver sa demande qui devra être validée par la DSI. | Obligatoire |  |

### Gestion de la configuration matérielle

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Toute modification de la configuration matérielle doit être réalisée en collaboration avec la DSI. | Obligatoire |  |

### Accès aux équipements

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| La DSI doit disposer de l'ensemble des comptes et mots de passe associés pour pouvoir accéder aux équipements.  Un compte « super-administrateur » doit donc être mis à disposition de la DSI. | Obligatoire |  |

### Comptes et authentification

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| La solution devra utiliser les comptes de connexions de l’Active Directory via LDAPS (LDAP avec SSL/TLS impérativement). Le non-respect de cette fonctionnalité devra être justifiée. | * Oui * Non |  |
| Si la solution n’utilise pas les comptes Active Directory de l’établissement, le prestataire doit justifier sa demande qui devra être validée par la DSI du CHR.  Dans ce cas le mot de passe de chaque compte doit respecter les règles suivantes :   * Changement du mot de passe à la première connexion * Ne pas contenir tout ou partie (de plus de 3 caractères) du nom du compte de l'utilisateur. * Remplacement annuel * Ne pas être identique au mot de passe précédemment utilisé * Contenir des caractères de trois des quatre catégories suivantes :   + Caractères majuscules   + Caractères minuscules   + Chiffres   + Caractères spéciaux   La taille minimale du mot de passe dépend du type de compte :   * Compte utilisateur = 10 caractères * Compte avec pouvoir = 12 caractères * Prestataire et compte de service = 15 caractères | * Oui * Non |  |
| Si la solution n’utilise pas de compte Active Directory ou ne respecte pas la politique de mot de passe citée précédemment, le prestataire devra s’engager contractuellement à se mettre en conformité dans un délai raisonnable (de 6 à 24 mois). | Obligatoire |  |
| Aucun compte générique ne sera actif, y compris pour l’administration par le prestataire. | * Oui * Non |  |
| Une matrice des habilitations sera à fournir selon le modèle remis par la DSI. | Obligatoire |  |

### Antivirus et EDR

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Tous les serveurs et les PC sont équipés de l’antivirus Windows Defender piloté par Microsoft EndPoint Configuration Manager. | Obligatoire |  |
| Si nécessaire, le prestataire devra fournir la liste des exclusions ciblées à mettre en place (pas d’exclusion d’un disque complet ni désactivation de l’antivirus). | Obligatoire |  |
| L’EDR Defender for Endpoint est activé et bloquera les potentielles activités suspectes. | Obligatoire |  |

### Chiffrement des flux

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| Les échanges seront chiffrés en TLS 1.2 minimum par l’intermédiaire de l’autorité de certification interne de l’établissement.  *A défaut le prestataire devra s’engager contractuellement à se mettre en conformité dans un délai raisonnable (de 6 à 24 mois).* | Obligatoire |  |
| Aucune application avec authentification et hébergeant des données sensibles ne sera acceptée avec un fonctionnement en http.  *A défaut le prestataire devra s’engager contractuellement à se mettre en conformité dans un délai raisonnable (de 6 à 24 mois).* | Obligatoire |  |

### Traçabilité des données

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| La solution doit permettre l’extraction des données suivantes :   * Horodatage des connexions et évaluation de durée * Opérations réalisées dans l’application * Attributions, modifications et révocation de droits des utilisateurs.   *A défaut le prestataire devra s’engager contractuellement à se mettre en conformité dans un délai raisonnable (de 6 à 24 mois).* | Obligatoire |  |
| La durée de rétention de ces éléments doit être à être minimum de 6 mois et de préférence de 1 an.  *A défaut le prestataire devra s’engager contractuellement à se mettre en conformité dans un délai raisonnable (de 6 à 24 mois).* | Obligatoire |  |

### Disponibilité des données

|  |  |  |
| --- | --- | --- |
| Engagement | Applicable | Commentaires |
| L'application doit travailler en temps réel. Toute donnée introduite et validée, est potentiellement disponible immédiatement sur l'ensemble des périphériques connectés. L'accès doit pouvoir être simultané à n'importe quelle donnée, à moins que ce ne soient des considérations de sécurité qui l'imposent. L'application devra proposer une gestion fine des accès concurrents en mise à jour, sans pour autant verrouiller une partie importante de la base. | * Oui * Non |  |

## Documents à fournir et enregistrements

### L'installation

L'installation matérielle et logicielle fera l'objet d'un procès-verbal de recette en accord avec la DSI.

Un mode-opératoire de « bonnes pratiques » sera fourni par le prestataire et contiendra au minimum :

* Installation du client
* Procédure changement de poste si besoin de récupérer des données/licences
* Coordonnées support et heures d'ouverture
* Emplacement contenant les données sensibles et les sources
* Synoptique de l’infrastructure applicative
* Flux réseaux
* Exclusions antivirus
* Éléments à superviser
* Matrice des habilitations sera à compléter selon le modèle remis par la DSI

### Enregistrements

#### Incidents

Tout incident matériel et logiciel sera consigné dans un document référençant la nature de l'incident, sa date et heure ainsi que sa résolution.

#### Interventions distantes

Conformément à la charte d’utilisation des technologies numériques pour le personnel externe, l’établissement met à disposition des accès distants nominatifs avec authentification à double facteur pour les interventions à distance.

Les accès sont tracés avec enregistrement des actions effectuées.

## Signature et engagement

|  |  |
| --- | --- |
| **Pour le Centre Hospitalier Régional de METZ-THIONVILLE** | **Pour le Prestataire** |
| Le Directeur du Système d’Information  À : le :  Signature et cachet | Nom : ……………………………  Prénom : …………………………  Fonction : ………………..………  À : le :  Signature et cachet |