|  |  |  |
| --- | --- | --- |
| LOGO_CHRMT | Processus | Référence : PROC/00026 |
| **Plan d’Assurance Sécurité SI (PAS)**  *Diffusion limitée : DSI et Prestataire de la solution* | Version : 01 |
| Date de publication : 29/12/2022 |
| Date prochaine révision :  08/12/2026 |

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** | **Relecteurs** | **Valideur** |
| **M. Cyril PIERRÉ**  Ingénieur Sécurité SI | **M. Albert CRUMBACH**  RSSI et DPO  **M. Mickael CHOPLIN**  Adjoint Directeur DSI | **M. Laurent KARMUSIK**  Directeur DSI |
| **08/12/2022 01 Création du document** | | |

# OBJET

Plan d’Assurance Sécurité (PAS) relatif à une prestation d’installation de maintenance et de maintien en condition opérationnelle d’une solution. Le PAS, document contractuel, décrit l'ensemble des dispositions spécifiques que le Prestataire s'engage à mettre en œuvre pour garantir le respect des exigences de sécurité SI du CHR.

# DOMAINE D’APPLICATION

Document contractuel entre le CHR et le prestataire.

# DEFINITIONS / ABREVIATIONS

* **CHR** : Centre Hospitalier Régional de METZ-THIONVILLE
* **DSI** : Direction du Système d’Information
* **PAS**: Plan d’Assurance Sécurité SI

# DOCUMENTS ASSOCIES

* **PROC/0649 :** Charte d’utilisation des technologies numériques pour le personnel externe au CHR METZ-THIONVILLE
* **PROC/00024 :** Conformité et prérequis techniques DSI
* **PROC/00028 :** Clauses contractuelles type RGPD Client (RT) - Prestataire (ST) 2022

# REFERENCES

* **RGPD** : Le Règlement (UE) 2016/679 ; Règlement Général sur la Protection des données
* **ANSSI :** recommandations et guide d’hygiène

# DEVELOPPEMENT

Table des matières

[1. Préambule 3](#_Toc256000000)

[2. Article 1 – Cadre général de la prestation 4](#_Toc256000001)

[3. Article 2 – Lieu d’exécution de la prestation 4](#_Toc256000002)

[4. Article 3 – Durée du contrat 4](#_Toc256000003)

[5. Article 4 – Interlocuteur du Prestataire sur la sécurité du système d’information 4](#_Toc256000004)

[6. Article 5 – Engagement sur les mesures de sécurité 6](#_Toc256000005)

[a. Gestion des risques 6](#_Toc256000006)

[b. Prise en compte de la sécurité au niveau des intervenants du Prestataire 7](#_Toc256000007)

[c. Prise en compte de la sécurité physique 8](#_Toc256000008)

[d. Sécurité des postes et des outils d’administration ou de maintenance 8](#_Toc256000009)

[e. Sécurité des interconnexions 9](#_Toc256000010)

[f. Identification, authentification et droits d’administration 10](#_Toc256000011)

[g. Situation de nomadisme 11](#_Toc256000012)

[h. Utilisation d’un système de stockage amovible pour ses actions d’administration ou de maintenance 11](#_Toc256000013)

[i. Journalisation des tâches planifiées et de maintenance 11](#_Toc256000014)

[j. Gestion des configurations et des changements 12](#_Toc256000015)

[k. Politique de sauvegarde / secours 13](#_Toc256000016)

[l. Gestion des incidents 13](#_Toc256000017)

[m. Organisation du Prestataire et gouvernance 14](#_Toc256000018)

[n. Audit de sécurité 14](#_Toc256000019)

[o. Territorialité de la prestation 16](#_Toc256000020)

[p. Protection des données à caractère personnel 16](#_Toc256000021)

[q. Architecture technique 16](#_Toc256000022)

[r. Liste des moyens techniques assurant une fonction de sécurité 17](#_Toc256000023)

[s. Matrice d’habilitation des intervenants du prestataire 17](#_Toc256000024)

[t. Liste des événements redoutés pris en compte par le Prestataire 17](#_Toc256000025)

[7. Signature et engagement 18](#_Toc256000026)

Plan d’Assurance Sécurité (PAS) relatif à une prestation d’installation, de maintenance et de maintien en condition opérationnelle d’une solution.

**ENTRE**

**Le Centre Hospitalier Régional de Metz-Thionville**

Etablissement public de santé

Dont le siège est 1, Allée du Château 57530 Ars-Laquenexy, à (57085) METZ CEDEX 03

M. Laurent KARMUSIK, Directeur du Système d’Information dûment habilitée à cet effet

Ci-après désigné le « CHR »

**ET**

**La Société** ………………………………………………………….

Dont le siège est ……………………………………………………

Représentée par ……………………………………………………, dûment habilité à cet effet

Ci-après désignée « Le Prestataire »

## Préambule

* 1. Le Prestataire est tenu de respecter l’ensemble des mesures du document « **PROC/00024 : Conformité et prérequis techniques DSI** »
  2. Le Prestataire est tenu de respecter l’ensemble des mesures du document « **PROC/00028 : Clauses contractuelles type RGPD Client (RT) - Prestataire (ST) 2022** »
  3. Ce document « **PROC/00026 : Plan d'Assurance Sécurité (PAS)** », document contractuel, décrit l'ensemble des dispositions spécifiques que le Prestataire s'engage à mettre en œuvre pour garantir le respect des exigences de sécurité du CHR.
  4. Ce Plan d’Assurance Sécurité engage le Prestataire ainsi que l’ensemble de ses sous-traitants. C’est le Prestataire qui en porte la responsabilité.
  5. Le PAS se substitue aux éventuelles clauses génériques de sécurité du Prestataire.
  6. Le Prestataire est tenu de mettre en œuvre les mesures techniques et d’organisation décrites dans le présent document.
  7. D’une manière générale, le Prestataire est tenu à une obligation de moyens pour protéger les données du CHR contre la destruction accidentelle ou illicite, la perte accidentelle, l’altération, la diffusion ou l’accès non-autorisé, notamment dans le cadre de la transmission de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.
  8. Le Prestataire est tenu à une obligation de conseil, de mise en garde et de recommandation en termes de sécurité et de mise à l’état de l’art.
  9. Le Prestataire s’engage à informer le CHR des risques d’une opération envisagée, des incidents éventuels ou potentiels (accès réalisé par des tiers non-autorisés, toute introduction de code malveillant, utilisation non conforme réalisée sur le système en place chez le Prestataire interconnecté avec le SI du CHR et de la mise en œuvre éventuelle d’actions correctrices ou de prévention.
  10. En cas d'arrêt des prestations confiées au Prestataire par le CHR, l'ensemble des matériels, logiciels et documentations confiés au Prestataire doivent être restitués. Le prestataire s’engage à apporter l’assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le CHR, ou par un autre prestataire de service. Le prestataire s’engage à restituer l’ensemble des données appartenant au CHR (clause de réversibilité).
  11. Dans le cadre d’un manquement grave par le prestataire à l’une des obligations de sécurité mises à sa charge dans le présent contrat, le CHR pourra le mettre en demeure de réparer ce manquement dans un délai donné. À l’issue de ce délai, si le manquement n’est pas réparé, le CHR pourra résilier de plein droit le contrat. De façon générale, tout manquement aux clauses doit entraîner des pénalités ou la résiliation, avec ou sans préavis.

**CECI EXPOSÉ IL A ÉTÉ CONVENU ET ARRÊTÉ CE QUI SUIT :**

## Article 1 – Cadre général de la prestation

La prestation, objet du contrat liant le Prestataire et le CHR, sur laquelle porte le présent Plan d’Assurance Sécurité vise à :

1. …………………………

2. …………………………

Jours et horaires de connexion (cochez les cases) :

*Support informatique du CHR disponible hors astreinte de 8h à 17h en jours ouvrés*

🞏 Jours ouvrés (8h – 17h)

🞏 Nuits (17h – 8h)

🞏 Week-ends (vendredi 17h au lundi 8h)

🞏 Jours fériés (veille 17h au lendemain 8h)

## Article 2 – Lieu d’exécution de la prestation

La prestation est réalisée sur les sites suivants (précisez l’adresse) :

……………………………………………………………………….

……………………………………………………………………….

……………………………………………………………………….

## Article 3 – Durée du contrat

Le présent contrat est prévu pour une durée de ………

## Article 4 – Interlocuteur du Prestataire sur la sécurité du système d’information

Dans le cadre du suivi de l’application du présent Plan d’Assurance Sécurité et des mesures de sécurité qui en découlent l’interlocuteur du Prestataire pour tout ce qui relève de la sécurité du système d’information concerné par le présent Plan d’Assurance Sécurité est :

M. / Mme …………………………

Fonction : …………………………

Coordonnées téléphoniques : ………………

Coordonnées électroniques : ………………

Le Prestataire s’engage sans délai à signaler au CHR tout changement d’interlocuteur ou tout changement de coordonnées de l’interlocuteur désigné.

## Article 5 – Engagement sur les mesures de sécurité

**Le Prestataire s’engage à respecter les mesures de sécurité définies ci-dessous si la mesure est applicable :**

### Gestion des risques

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-a.1 | Le Prestataire garantit avoir identifié avec précision les risques liés à l’usage des systèmes d’information nécessaires à la réalisation de la prestation définie à l’article 1 du présent document. Les risques ainsi identifiés permettent de déterminer les mesures nécessaires à leur réduction. Cette appréciation des risques est, à minima, revue annuellement par le Prestataire.  Le Prestataire doit disposer d’un document décrivant les risques identifiés et les mesures de sécurité mises en œuvre ou prévues pour les réduire. Ce document pourra être transmis au CHR sur demande.  Le chapitre ’T’ de ce document « [Liste des évènements redoutés pris en compte par le Prestataire](#_Liste_des_événements)» précise les principaux évènements redoutés par le prestataire dans le cadre de la prestation proposée au CHR et les mesures de sécurité prévues pour limiter les risques de survenance. | Obligatoire |  |
| Eng-a.2 | Le Prestataire dispose d’une politique de sécurité (PSSI) du SI qu’il met en œuvre dans le cadre de la prestation définie à l’article 1 du présent document.  Les directives et les règles de sécurité qui découlent de la PSSI sont conformes aux bonnes pratiques énoncées dans les normes ISO 2700x en vigueur et par les autorités compétentes notamment l’ANSSI, la CNIL et l’ANS. Ces directives permettre de prévenir et de limiter les risques identifiés par le Prestataire (cf. Eng-a.1). A minima, le Prestataire doit appliquer le guide d’hygiène informatique de l’ANSSI au système d’information qu’il met en œuvre dans le cadre de la prestation définie à l’article 1 du présent document.  La PSSI spécifique du prestataire pourra être transmis au CHR sur demande. | 🞏 Oui  🞏 Non |  |
| Eng-a.3 | Le Prestataire s’engage à évaluer en permanence la sécurité de sa solution dans l’écosystème CHR afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour faire face aux nouveaux risques de sécurité ou aux résultats obtenus à l'issue de ses propres examens périodiques.  Le Prestataire s’engage à notifier au CHR tout changement qu'il considère comme étant un abaissement du niveau de sécurité à partir de la date de prise d'effet du présent contrat, en lui communiquant des informations sur la nature du changement, la finalité du changement et sa date de prise d’effet des mesures correctives. | 🞏 Oui  🞏 Non |  |
| Eng-a.4 | Le Prestataire s’engage à fournir tous les éléments permettant l’homologation de la sécurité de sa solution par le CHR. | Obligatoire |  |
| Eng-a.5 | Le Prestataire doit souscrire une assurance couvrant les éventuels dommages causés au CHR et notamment à son système d’information dans le cadre de sa prestation, en détaillant le niveau de garantie.  Une attestation d’assurance pourra être remise au CHR sur demande. | 🞏 Oui  🞏 Non |  |

### Prise en compte de la sécurité au niveau des intervenants du Prestataire

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-b.1 | Le Prestataire dispose d’un annuaire complet et récent de tous ses collaborateurs intervenant dans le cadre de la prestation. Cet annuaire doit préciser les rôles et responsabilités de chaque intervenant et son périmètre d’intervention.  L’annuaire doit être envoyé au CHR en début de prestation, tous les 6 mois et sur demande.  Le chapitre ‘S’ de ce document « [Matrice d’habilitation des personnels du prestataire](#_Matrice_d’habilitation_des) » précise la matrice d’habilitation des personnels du Prestataire au moment de la signature du présent contrat. Le prestataire s’engage à mettre à jour cette matrice dès que nécessaire et à la remettre au CHR sur demande. | Obligatoire |  |
| Eng-b.2 | Tous les collaborateurs du Prestataire amenés à intervenir dans le cadre de la prestation signent un engagement individuel de confidentialité « Charte d’utilisation des technologies numériques pour le personnel externe au CHR Metz-Thionville ». Ces engagements individuels de confidentialité seront transmis au CHR.  Dans la mesure où la prestation nécessite le recours à la sous-traitance ou à la cotraitance, le Prestataire s’engage à imposer par écrit un engagement individuel de confidentialité et à en justifier au CHR à toute demande ou lors d’un audit. | Obligatoire |  |
| Eng-b.3 | Le présent PAS (ou un document de politique de sécurité regroupant les exigences de sécurité liées aux prestations réalisées et les moyens mis en œuvre pour y répondre) doit être diffusé à l’ensemble des intervenants.  Tous les intervenants identifiés dans l’annuaire doivent suivre une session de sensibilisation à la sécurité rappelant les exigences sécurité de la prestation et les bonnes pratiques de sécurité. La liste des intervenants ayant suivi une session de sensibilisation doit être disponible sur demande du CHR. | 🞏 Oui  🞏 Non |  |
| Eng-b.4 | Le Prestataire s’engage à informer sans délai le CHR de tout départ d’un intervenant du Prestataire.  Dans ce cas, il s’engage a mettre à jour la matrice d’habilitation lié à la prestation fournie au CHR. | 🞏 Oui  🞏 Non |  |

### Prise en compte de la sécurité physique

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-c.1 | Le Prestataire s’engage à intégrer les éléments de sécurité physique dans l’appréciation des risques conformément au niveau de sécurité requis par la prestation définie à l’article 1 du présent document. | 🞏 Oui  🞏 Non |  |
| Eng-c.2 | Le Prestataire s’engage à documenter et mettre en œuvre des procédures relatives au travail en zones sensibles. Il doit communiquer ces procédures aux intervenants concernés. | 🞏 Oui  🞏 Non |  |
| Eng-c.3 | Le Prestataire s’engage à documenter et mettre en œuvre des mesures permettant de s’assurer que les conditions – matérielles et logicielles – d’installation, de maintenance et d’entretien des équipements du système d’information du service fourni au CHR sont compatibles avec les exigences de confidentialité et de disponibilité du CHR. | 🞏 Oui  🞏 Non |  |

### Sécurité des postes et des outils d’administration ou de maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-d.1 | Le Prestataire s’engage à s’assurer que les postes des administrateurs ne disposent que des logiciels et fonctions nécessaires au besoin opérationnel de la solution. | 🞏 Oui  🞏 Non |  |
| Eng-d.2 | Le Prestataire s’engage à s’assurer que les postes d’administration disposent d’un dispositif de filtrage réseau local activé et configuré pour n’autoriser que les connexions répondant strictement au besoin opérationnel. | 🞏 Oui  🞏 Non |  |
| Eng-d.3 | Le Prestataire est responsable des outils d’administration utilisés par ses administrateurs et de leur utilisation dans des conditions de sécurité (précautions d’usage, maîtrise de la configuration, etc.) pour la réalisation de la prestation. Pour cela, le Prestataire s’engage à s’assurer que ces outils sont pris en compte dans le maintien en conditions de sécurité. | 🞏 Oui  🞏 Non |  |
| Eng-d.4 | Le Prestataire s’engage à s’assurer que les outils de gestion des configurations qu’il met en œuvre garantissent l'intégrité et la traçabilité des éléments qu'ils contiennent et suivant les besoins, la confidentialité. | 🞏 Oui  🞏 Non |  |
| Eng-d.5 | Le Prestataire s’engage à s’assurer que les serveurs outils d'administration sous sa responsabilité n’ont aucun accès à Internet direct en dehors de celui fourni par le CHR. | 🞏 Oui  🞏 Non |  |
| Eng-d.6 | Le Prestataire s’engage à accéder aux outils d’administration en utilisant des protocoles permettant l’authentification et le chiffrement au niveau applicatif en conformité avec les guides de l’ANSSI (TLS et SSH), le cas échéant selon les protocoles utilisés, ou à défaut au niveau IP en conformité avec le guide IPSEC de l’ANSSI. | 🞏 Oui  🞏 Non |  |
| Eng-d.7 | Le Prestataire s’engage à accéder aux ressources administrées en utilisant la solution Bastion d’accès distant sécurisé du CHR. | 🞏 Oui  🞏 Non |  |
| Eng-d.8 | Le Prestataire s’engage à fournir au CHR les éléments nécessaires afin d’activer et configurer un dispositif de filtrage réseau local sur les serveurs outils d’administration pour n’autoriser que les connexions répondant strictement au besoin opérationnel de la solution (cartographie/matrice des flux applicatifs et réseaux). Seuls les pares-feux du CHR sont autorisés. | 🞏 Oui  🞏 Non |  |
| Eng-d.09 | Le Prestataire s’engage à durcir les configurations système et applicative des serveurs outils nécessaire à la réalisation de la prestation afin de renforcer la sécurité SI. | 🞏 Oui  🞏 Non |  |
| Eng-d.10 | Le Prestataire s’engage à s’assurer que les serveurs outils d’administration ne disposent que des logiciels et fonctions nécessaires au besoin opérationnel du service. | 🞏 Oui  🞏 Non |  |
| Eng-d.11 | Le Prestataire s’engage à tenir à jour l’inventaire de l’ensemble des logiciels et micrologiciels mettant en œuvre la prestation de service. Cet inventaire doit identifier pour chaque logiciel, sa version et les équipements sur lesquels le logiciel est installé.  Le Prestataire doit fournir une cartographie logique et physique. | 🞏 Oui  🞏 Non |  |
| Eng-d.12 | Le Prestataire s’engage à installer et maintenir les dispositifs du service dans des versions stables et à jour de leurs correctifs de sécurité. Les versions installées doivent être des versions supportées sauf si celles-ci empêchent la réalisation de la prestation de service.  Le Prestataire doit s’assurer de l’authenticité et de l’intégrité des mises à jour téléchargées auprès des sources de mise à jour. | 🞏 Oui  🞏 Non |  |
| Eng-d.13 | Le Prestataire s’engage à documenter et réaliser une veille sur les vulnérabilités, les mises à jour de sécurité et les mesures de réduction des risques concernant les ressources du système d’information de la prestation de service. | 🞏 Oui  🞏 Non |  |
| Eng-d.14 | Les postes et les outils d’administration doivent comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants notamment dans le cas d’utilisation de supports amovibles.  Si le dispositif ne peut pas comporter de solution antivirus (automate…), la DSI doit être informée pour durcir la sécurité SI de l’écosystème de la solution afin de prévenir toute contagion. Dans ce cas, l’utilisation de périphérique externe de stockage est interdite. | 🞏 Oui  🞏 Non |  |

### Sécurité des interconnexions

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-e.1 | Lorsque le Prestataire souhaite transmettre un fichier sensible pouvant porter atteinte au CHR, celui-ci doit être chiffré au travers d’un flux sécurisé avec traçabilité, accessible par des utilisateurs habilités. | Obligatoire |  |
| Eng-e.2 | Lorsque le CHR souhaite déposer un fichier chez le Prestataire, ce dernier doit restreindre les accès aux seules personnes habilitées. | Obligatoire |  |
| Eng-e.3 | L’interconnexion réseau entre le Prestataire et le CHR s’appuie sur un flux sécurisé et strictement limité aux besoins opérationnels transitant par un dispositif de filtrage (exemple IPSec, https …). | Obligatoire |  |
| Eng-e.4 | Le prestataire doit s’assurer que tous les flux de sa solution à destination d’Internet transitent par la solution de filtrage Web du CHR. | Obligatoire |  |
| Eng-e.5 | Le prestataire doit s’assurer que seuls les flux correspondant au strict besoin opérationnel de la solution sont autorisés et transitent par des dispositifs de filtrages. | Obligatoire |  |

### Identification, authentification et droits d’administration

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-f.1 | Le Prestataire s’engage à s’interfacer à l’annuaire centralisé (Active Directory).  Le Prestataire doit respecter les règles de cloisonnement entre compte administrateur et compte utilisateur. | 🞏 Oui  🞏 Non |  |
| Eng-f.2 | Le Prestataire s’engage à attribuer des comptes administrateurs nominatifs. | 🞏 Oui  🞏 Non |  |
| Eng-f.3 | Le Prestataire s’engage à s’assurer que les comptes de service ne sont utilisés que pour répondre à un besoin opérationnel spécifique et sont effectifs sur le seul périmètre associé à ce besoin. | Obligatoire |  |
| Eng-f.4 | Le Prestataire s’engage à s’assurer que les mots de passe portés à la connaissance des administrateurs sont stockés exclusivement dans un outil de gestion sécurisée des mots de passe.  Le Prestataire s’engage à respecter la « Politique de gestion des comptes et des mots de passe » du CHR | Obligatoire |  |
| Eng-f.5 | Le Prestataire s’engage à ne pas utiliser de compte générique et à supprimer les comptes par défaut de la solution. | Obligatoire |  |
| Eng-f.6 | Le Prestataire s’engage à désactiver les comptes dès le départ ou la suspension d'un administrateur ; ces comptes doivent être supprimés au terme d'un délai maximal d’un mois. | Obligatoire |  |
| Eng-f.7 | Le Prestataire s’engage à ce que les mots de passes soient chiffrés. Aucun mot de passe ne doit apparaître en clair (par exemple dans une procédure, dans un fichier de configuration, dans un script, dans une URL ou dans une base de données). | 🞏 Oui  🞏 Non |  |
| Enf-f-8 | Le Prestataire s’engage à fournir un compte d’administrateur nominatif par composant de sa solution à la DSI du CHR (application, serveur, base de données, équipement …). En cas de départ de la personne, son compte sera supprimé et un nouveau créé pour son remplaçant. | Obligatoire |  |

### Situation de nomadisme

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-g.1 | Le Prestataire s’engage à mettre en œuvre et tenir à jour une liste de ses administrateurs nomades. | 🞏 Oui  🞏 Non |  |
| Eng-g.2 | Le Prestataire s’engage à sensibiliser aux bonnes pratiques de sécurité liées au nomadisme les administrateurs possédant un poste nomade.  Le prestataire s’engage à ce que ces postes nomades soient chiffrés. | 🞏 Oui  🞏 Non |  |
| Eng-g.3 | Le Prestataire s’engage à bloquer l’accès du poste d’administration ou de maintenance nomade au reste du système d’information du service sans délai après sa déclaration de perte ou de vol. | 🞏 Oui  🞏 Non |  |

### Utilisation d’un système de stockage amovible pour ses actions d’administration ou de maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-h.1 | Le Prestataire s’engage à dédier physiquement un ou plusieurs systèmes de stockage amovibles à la prestation réalisée pour le compte du CHR. | 🞏 Oui  🞏 Non |  |
| Eng-h.2 | Le Prestataire s’engage à réaliser une analyse antivirus sur tout système de stockage amovible avant chaque connexion sur le système d’information du CHR. | 🞏 Oui  🞏 Non |  |

### Journalisation des tâches planifiées et de maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-i.1 | Le Prestataire s’engage à s'assurer que les actions de support réalisées par les scripts sont journalisées. Les événements journalisés doivent inclure :  - le compte ayant lancé le script de support ;  - les comptes ayant exécuté les actions de support ;  - l’horodatage des actions de support ;  - les ressources administrées concernées par les scripts de support ;  - la description des actions de support réalisées et les résultats du script de support. | 🞏 Oui  🞏 Non |  |
| Eng-i.2 | Le Prestataire s’engage à s'assurer que les sauvegardes des fichiers journaux sont hébergées dans le système d'information du CHR. | 🞏 Oui  🞏 Non |  |
| Eng-i.3 | Le Prestataire s’engage à s'assurer que la durée de rétention des journaux est de 1 an minimum. | 🞏 Oui  🞏 Non |  |
| Eng-i.4 | Tous les systèmes du Prestataire (postes de travail, serveurs et composants d’infrastructure) doivent enregistrer les accès réussis, les tentatives d’accès et les fermetures de session.  Les traces générées doivent contenir au minimum les informations suivantes :   * La date et l’heure de l’événement * La typologie de l’événement (par ex : l’accès) et le résultat de l’événement (succès, échec) ; * L’auteur de l’action ou à l’origine de l’événement (identifiant du compte) ; * L’identification de la ressource à l’origine de l’événement (adresse IP, nom du système, nom de l’application ou du processus) ; * L’identification du système et des applications accédés (nom, adresse IP, protocole, port).   En cas de malversation ou d’incident, les traces générées doivent permettre de remontrer jusqu’aux intervenants et aux ressources utilisées. | 🞏 Oui  🞏 Non |  |
| Eng-i.5 | Les traces générées par les différents systèmes doivent faire l’objet d’une analyse périodique. Toutes les anomalies doivent faire l’objet d’une investigation et, si nécessaire, d’une gestion d’incident. | 🞏 Oui  🞏 Non |  |
| Eng-i.6 | Toutes les traces générées dans le cadre de la prestation doivent pouvoir être mises à disposition, sans aucune modification et en préservant leur intégrité, sur demande du CHR ou d’un auditeur mandaté par le CHR. | 🞏 Oui  🞏 Non |  |
| Eng-i.7 | Toutes les traces générées dans le cadre de la prestation devront être conservées pendant 1 an minimum.  Des mesures de protection et de contrôle doivent être mises en œuvre afin de s’assurer de la sécurité des traces (intégrité, disponibilité, accès sécurisé, conditions de rétention). | 🞏 Oui  🞏 Non |  |

### Gestion des configurations et des changements

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-j.1 | Le Prestataire s’engage à ce que toute demande de changement relative à un progiciel déployé sur le SI du CHR fasse l'objet d'une validation du CHR et doit s’assurer de la présence de toute sauvegarde permettant de revenir à la situation antérieure en cas de problème. | Obligatoire |  |
| Eng-j.2 | Le Prestataire s’engage à tenir à jour les versions des progiciels déployés sur le SI du CHR dont il a la charge avec la validation du CHR. | 🞏 Oui  🞏 Non |  |
| Eng-j.3 | Le Prestataire s’engage à mettre à jour les versions de systèmes et les correctifs à apporter, ainsi que les paramétrages des publications de sécurité. | 🞏 Oui  🞏 Non |  |
| Eng-j.4 | Le Prestataire s’engage à interdire l’ajout ou la création d’outils ou d’utilitaires sur les progiciels déployés sur le SI du CHR sans avoir obtenu une autorisation du CHR. | Obligatoire |  |
| Eng-j.5 | Le Prestataire s’engage à systématiquement décrire dans une documentation (obligatoire avant tout passage en production) les nouvelles fonctionnalités (ou changements de fonctionnalités) liées à un nouveau système ou à une nouvelle version majeure des progiciels déployés sur le SI du CHR. | Obligatoire |  |
| Eng-j.6 | Le Prestataire s’engage à tenir à jour les paramétrages de sécurité et règles de configuration déployées sur les progiciels déployés sur le SI du CHR et les fournir sur demande. | 🞏 Oui  🞏 Non |  |
| Eng-j.7 | Le Prestataire s’engage à intégrer dans la procédure de gestion des changements l'obligation de tests de non-régression. | 🞏 Oui  🞏 Non |  |

### Politique de sauvegarde / secours

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-k.1 | Le Prestataire s’engage à s’assurer de la consistante de la sauvegarde de l’ensemble de sa solution (données, paramétrage, configuration…). | Obligatoire |  |
| Eng-k.2 | Le Prestataire s’engage à s’assurer de la continuité de service des composants de sa solution. | 🞏 Oui  🞏 Non |  |

### Gestion des incidents

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-l.1 | Des outils et des procédures de gestion des incidents/alertes de sécurité (déclenchement, responsables/organisation interne, déroulement, suivi de la prise en charge, diffusion de l’alerte…) doivent être mise en place pour tout événement susceptible d’affecter la sécurité des informations et du SI administrés (vol, perte, attaque informatique, intrusion physique, arrêt d’un service de sécurité sur un poste de travail, etc.). | 🞏 Oui  🞏 Non |  |
| Eng-l.2 | Le Prestataire s’engage à analyser les événements pouvant être révélateurs de comportements anormaux ou d'actions illicites et à mettre en place des points ou indicateurs de surveillance en conséquence. | 🞏 Oui  🞏 Non |  |
| Eng-l.3 | Le Prestataire s’engage à surveiller les traces, logs et journaux afin de faire une analyse approfondie des événements pouvant avoir un impact sur la sécurité (connexions refusées, reconfigurations, évolutions de performances, accès à des informations ou des outils sensibles, etc.) | 🞏 Oui  🞏 Non |  |
| Eng-l.4 | Le Prestataire s’engage à signaler sans délai tout événement pouvant être révélateurs de comportements anormaux ou d'actions illicites ou tout événement pouvant avoir un impact sur la sécurité. | 🞏 Oui  🞏 Non |  |
| Eng-l.5 | Le Prestataire s’engage à informer le CHR de tout incident touchant la sécurité (vol, perte, attaques informatiques de tout type), en précisant :   * La nature de l’incident ; * Les mesures immédiates prises pour contourner ou résoudre l’incident ; * Le plan d’action proposé.   En cas d’intrusion logique, l’équipe d’exploitation du CHR pourra à tout moment couper la liaison entre les sites du Prestataire et le site du CHR, afin de mener les investigations nécessaires et prendre les mesures appropriées. Dans ces conditions, le CHR pourra à tout moment demander au Prestataire les éléments de journalisation et de trace délivrés par les équipements de sécurité. | 🞏 Oui  🞏 Non |  |

### Organisation du Prestataire et gouvernance

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-m.1 | Le Prestataire s’engage à être liés contractuellement avec ses administrateurs ou avec un de ses sous-traitants dans le cas de la sous-traitance d’une partie de son activité | 🞏 Oui  🞏 Non |  |
| Eng-m.2 | Le Prestataire s’engage à mettre en œuvre un processus disciplinaire applicable à l’ensemble des personnes impliquées dans la fourniture du service ayant enfreint la politique de sécurité. | 🞏 Oui  🞏 Non |  |
| Eng-m.3 | Le Prestataire s’engage à élaborer et mettre en œuvre un plan de sensibilisation de son personnel à la sécurité des systèmes d’information et des mesures de sécurité associées. | 🞏 Oui  🞏 Non |  |
| Eng-m.4 | Le Prestataire s’engage à documenter et mettre en œuvre un plan de formation concernant la sécurité de l’information adapté au service et aux missions des personnels. | 🞏 Oui  🞏 Non |  |
| Eng-m.5 | Le Prestataire s’engage à élaborer et mettre à disposition des intervenants les modes-opératoires dans le cadre de la délivrance du service. | 🞏 Oui  🞏 Non |  |
| Eng-m.6 | Le Prestataire s’engage à documenter et réaliser une veille sur les vulnérabilités, les mises à jour de sécurité et les mesures de réduction des risques concernant les ressources des systèmes d’information administrés. | 🞏 Oui  🞏 Non |  |

### Audit de sécurité

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-n.1 | Afin de s’assurer de la bonne application des dispositions des mesures de sécurité définie dans le présent document, le Prestataire autorise le CHR (ou un auditeur mandaté par le CHR) à effectuer des audits de sécurité planifiés (revues de sécurité de code applicatif, tests d’intrusion, audits d’architecture et de configuration, audit organisationnel) avant le démarrage, pendant ou à l’issue de la prestation.  Dans le cadre de ces audits, le Prestataire s’engage à mettre en œuvre tous les moyens techniques et organisationnels visant à permettre la réalisation de ces audits. Il s’engage à s’assurer notamment de la disponibilité des intervenants pour fournir toutes les informations nécessaires aux auditeurs, ainsi que de la gestion des accès aux locaux ou aux composants utilisés pour les prestations. | 🞏 Oui  🞏 Non |  |
| Eng-n.2 | Le Prestataire s’engage à assurer à son niveau des contrôles ou audits de sécurité périodiques, afin de s’assurer de la bonne application des exigences, des procédures de sécurité et de la protection des informations sensibles.  Ces contrôles ou audits doivent couvrir les domaines techniques et organisationnels. Une synthèse des rapports d’audits doit être fournie au CHR sur demande. | 🞏 Oui  🞏 Non |  |
| Eng-n.3 | Tous les contrôles ou audits réalisés par une société externe, mandatée par le Prestataire et incluant le périmètre de la prestation, doit être soumis à l’accord du CHR. Un accord de confidentialité doit être signé par la société externe.  Les résultats de ces contrôles ou audits et les plans d’actions associés devront être communiqués au CHR. | 🞏 Oui  🞏 Non |  |
| Eng-n.4 | Le Prestataire autorise le CHR à faire effectuer des recherches de vulnérabilités automatisées sur le système installé au CHR. Ces tests permettront d’évaluer la vulnérabilité du SI du Prestataire et pourront être réalisés avant la mise en protection et de façon périodique.  Une demande sera envoyée au Prestataire, afin qu’il précise les dates et plages horaires autorisés pour mener ces tests. | Obligatoire |  |
| Eng-n.5 | Le Prestataire autorise le CHR, ou tout autre Prestataire choisi par le CHR, sous réserve de non concurrence, à effectuer des tests d’intrusion sur le système installé au CHR. | Obligatoire |  |
| Eng-n.6 | Dans l'hypothèse où le rapport d'audit ou la réalisation des tests d’intrusion ferait apparaître un manquement du Prestataire à ses obligations contractuelles, le Prestataire s’engage à mettre en œuvre les mesures correctives jugées nécessaires dans les délais requis selon la nature du manquement concerné.  A défaut de voir le Prestataire remédier en temps voulu aux manquements constatés, le CHR se réserve le droit de résilier le Contrat selon les conditions de résiliation définies dans ledit Contrat. | Obligatoire |  |

### Territorialité de la prestation

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-o.1 | Le Prestataire s’engage à héberger et traiter les données relatives au service d’administration et de maintenance sécurisées exclusivement au sein d’un État de l’Union Européenne et avec la garantie impérative de ne pas être soumis à d’autre législation que celles de l’Union Européenne. | 🞏 Oui  🞏 Non |  |
| Eng-o.2 | Le Prestataire s’engage à communiquer la localisation de l’hébergement de données concernant le CHR. | Obligatoire |  |

### Protection des données à caractère personnel

|  |  |  |  |
| --- | --- | --- | --- |
| Réf. | Engagement | Applicable | Commentaires  *Obligatoire si non applicable* |
| Eng-p.1 | Le Prestataire s’engage à respecter les obligations qui s’impose à lui en tant que sous-traitant au titre de l’art. 28 du RGPD pour les activités de traitement concernées par la prestation.  Ces engagements sont contractualisés dans un document conforme aux directives des autorités compétentes (Clauses contractuelles types de la CNIL). | Obligatoire |  |

### Architecture technique

Obligatoire

L’architecture technique mise en œuvre par le Prestataire dans le cadre de la prestation est présentée dans le croquis suivant :

**Synoptique d’architecture et cartographie des flux à insérer**

### Liste des moyens techniques assurant une fonction de sécurité

|  |  |
| --- | --- |
| Fonction | Moyens techniques opérationnels |
| Authentification des administrateurs (authentification AD, Bastion, MFA…) | ***A compléter*** |
| Lutte contre les codes malveillants | ***A compléter*** |
| Lutte contre les intrusions informatiques | ***A compléter*** |
| Détection des incidents de sécurité | ***A compléter*** |
| Surveillance | ***A compléter*** |
| Traçabilité des opérations réalisées par les administrateurs | ***A compléter*** |
| Sécurité des échanges | ***A compléter*** |
| Sécurité des données stockées | ***A compléter*** |
| Chiffrement des données utilisées par les administrateurs | ***A compléter*** |
| *Autre* | ***A compléter*** |

### Matrice d’habilitation des intervenants du prestataire

Le Prestataire doit fournir une liste de ses intervenants habilités. A chaque mouvement de personnel (création, modification, suppression), il devra informer le CHR.

Chaque intervenant devra signer la « **PROC/0649 :** Charte d’utilisation des technologies numériques pour le personnel externe au CHR METZ-THIONVILLE »

### Liste des événements redoutés pris en compte par le Prestataire

Le tableau ci-dessous détaille les mesures prisent en compte par le prestataire pour protéger son propre système d’information et éviter ainsi un rebond malveillant vers le système d’information du CHR.

|  |  |  |
| --- | --- | --- |
| Evénement redouté | Description | Mesures prévues pour réduire le risque |
| Intrusion dans le SI du Prestataire avec rebond potentiel vers le SI du CHR | ***A compléter*** | ***A compléter*** |
| Attaque virale sur le poste de travail des personnels du prestataire | ***A compléter*** | ***A compléter*** |
| Fuite de données collectées dans le cadre de la prestation | ***A compléter*** | ***A compléter*** |
| Attaque de déni de service | ***A compléter*** | ***A compléter*** |
| Malveillance par le personnel du Prestataire | ***A compléter*** | ***A compléter*** |
| Erreur humaine | ***A compléter*** | ***A compléter*** |
| *A compléter* | ***A compléter*** | ***A compléter*** |

## Signature et engagement

Fait à ……………………,

Le ……………….………

En deux exemplaires originaux.

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