|  |  |  |
| --- | --- | --- |
| LOGO_CHRMT | PROCEDURE | Référence : PROC/0649 |
| **Charte d’utilisation des technologies numériques pour le personnel extérieur au CHR METZ-THIONVILLE** | Version : 01 |
| Date de publication : 29/12/2022 |
| Date de prochaine révision : 09/06/2026 |

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(s)** | **Relecteur(s)** | **Valideur(s)** |
| Nom | **Cyril PIERRÉ**  Ingénieur Sécurité SI | **M. Albert CRUMBACH**  RSSI et DPO | **M. Laurent KARMUSIK**  Directeur DSI |
| Date | 25/05/2022 | 30/05/2022 | 30/05/2022 |
| Signature |  |  |  |

# OBJET

Le Système d’Information constitue une ressource stratégique indispensable pour le CHR dans la conduite de son activité. Ce Système d’Information étant exposé à de nombreux risques en termes de sécurité (accidents, erreurs, malveillances, etc.), une Politique de Sécurité du Système d’Information (PSSI) a été élaborée pour définir les principes et règles de sécurité, et préciser les rôles et responsabilités de chacun. La présente charte s’inscrit dans le cadre de la PSSI. Elle est de ce fait un document de référence pour l’établissement.

Dans cet objectif, la présente charte, relative à l’accès et à l’utilisation des ressources du Système d’Information du CHR, précise les règles et précautions que les personnels extérieurs au CHR doivent respecter afin de garantir un usage fiable et sécurisé des ressources du Système d’Information.

En signant cette charte, le personnel extérieur reconnait en avoir pris connaissance et s’engage librement à en appliquer strictement le contenu.

L’accès aux services est conditionné à l’acceptation du contrat et des annexes Sécurité du SI et des clauses RGPD contractualisés entre l’entreprise et l’établissement.

# DOMAINE D’APPLICATION

Cette charte s’applique à tous les éléments du Système d’Information mis à la disposition des personnels extérieurs au CHR par le CHR (matériels fixes ou nomades, logiciels, systèmes de communication en interne ou en extérieur, etc.), ainsi qu’aux données stockées ou véhiculées par ces éléments.

Elle s’adresse à tout personnel extérieur autorisé à accéder, traiter ou utiliser des ressources du Système d’Information du CHR le cadre de son activité professionnelle.

Cette charte complète le contrat signé avec le personnel extérieur ainsi que les annexes liées à la protection des données (clauses RGPD) et à la sécurisation du Système d’Information (Plan Assurance Sécurité) mais ne s’y substitue pas. Elle n’a pas pour objet de couvrir de façon exhaustive tous les cas de figure possibles, mais plutôt de fixer les principes généraux d’utilisation : c’est donc à l’esprit de ces principes que le personnel extérieur devra se conformer dans des situations non envisagées.

# DEFINITIONS ABREVIATIONS

* **CHR** : Centre Hospitalier Régional de METZ-THIONVILLE
* **DSI** : Direction du Système d’Information
* **PAS :** Plan d’Assurance Sécurité
* **Personnel extérieur :** Personnel non employé par l’établissement et sous convention ou contrat (exemples : prestataires, sous-traitants, fournisseurs, partenaires …)
* **RGPD :** Règlement Général sur la Protection des données

# DOCUMENTS ASSOCIES

-

# REFERENCES

* **RGPD** : Le Règlement (UE) 2016/679 ; Règlement Général sur la Protection des données
* **Loi Informatique et Liberté** du 6 janvier 1978
* **Recommandations ANSSI :** Guide authentification multifacteur et mots de passe de l’ANSSI

# DEVELOPPEMENT

Table des matières

[1. Règles de sécurité à respecter 2](#_Toc256000000)

[a. Confidentialité des données 2](#_Toc256000001)

[b. Protection des accès aux SI 3](#_Toc256000002)

[c. Protection des comptes et droits d’accès 3](#_Toc256000003)

[d. Déclaration des vulnérabilités et incidents 4](#_Toc256000004)

[e. Traçabilité et contrôle 4](#_Toc256000005)

[f. Engagement de confidentialité 4](#_Toc256000006)

[2. Acte d’engagement personnel 5](#_Toc256000007)

## Règles de sécurité à respecter

Chaque personnel extérieur s’engage à respecter les règles de sécurité définies par le CHR, incluant les règles dictées dans la Charte d'utilisation des technologies numériques.

### Confidentialité des données

Le personnel extérieur s’engage à garantir en toutes circonstances la confidentialité des informations du CHR.

Le personnel extérieur s’engage à ne prendre connaissance des informations du CHR ou à n’y donner accès que dans le cadre de ses attributions ou sur demande d’une personne habilitée du CHR.

Le personnel extérieur veille à ne pas prendre connaissance des données de santé ou des données personnelles d’utilisateurs (messagerie, fichiers sur le poste de travail, identifiant et mot de passe, etc.) et à n’autoriser personne à y accéder, sauf demande formelle par une personne habilitée.

Il veille à ne pas utiliser les documents et informations obtenus ou produits à d’autres fins que celles prévues au contrat et à ne divulguer aucune information sensible sans autorisation du CHR, et ce y compris au sein de sa société.

Le personnel extérieur s’engage à ne prendre aucune copie des documents, données et supports d'informations qui lui sont confiés ou auxquels il a accès, à l’exception de celles nécessaires à l’exécution de la prestation prévue au contrat ou de celles explicitement autorisées par le RSSI du CHR.

Il s’assure de prendre toutes les mesures nécessaires pour assurer la confidentialité des informations qui lui sont confiées pendant la durée du contrat.

À la fin de contrat ou de son intervention, il procède à la destruction de tous les documents physiques ou numériques contenant des données du CHR.

### Protection des accès aux SI

Le personnel extérieur s’engage à utiliser les seuls moyens d’accès au SI, mis à disposition ou validés par le CHR, qu’il s’agisse d’accès depuis le site du CHR ou à distance. Il respecte les procédures et règles communiquées par le CHR pour accéder au SI.

Le personnel extérieur ne pourra accéder au Système d’Information qu’à partir du moment ou les ouvertures d’accès auront été réalisés selon la procédure interne en vigueur.

**Chaque connexion est tracée et horodatée : elle fait également l’objet d’un enregistrement vidéo opposable.**

L’accès distant se fait avec une authentification multifacteur avec des comptes nominatifs pour chaque intervenant.

Il veille à ne pas outrepasser ni tenter de contourner les mesures de sécurité et le contrôle d’accès en place, pour quelque raison que ce soit.

Le personnel extérieur veille à ne pas connecter de matériel non fourni par le CHR sur le réseau interne du CHR sans autorisation préalable selon la procédure interne en vigueur disponible auprès du responsable du CHR l’accueillant.

Lors de ses accès aux salles informatiques des établissements du CHR, le personnel extérieur respecte les règles suivantes :

* Toute intervention dans les salles informatiques doit faire l’objet d’une validation préalable formelle de la DSI l’établissement ;
* Lorsqu’une intervention sur site est nécessaire en dehors des heures ouvrées, le personnel extérieur doit se présenter à l’accueil de l’établissement qui contactera le poste de Sécurité ;
* L’intervention sera, dans la mesure du possible, encadrée par une personne habilitée du CHR ;
* Sur demande de la DSI de l’établissement, le personnel extérieur doit fournir un rapport d’intervention détaillant les opérations réalisées, exhaustif et officiel.

Lors de ses accès à distance au SI du CHR, le personnel extérieur respecte les règles suivantes :

* Toute intervention sur le SI doit se faire dans le strict respect des règles définies par le CHR et dans le contrat ;
* Sur demande de la DSI de l’établissement, le personnel extérieur doit fournir un rapport d’intervention détaillant les opérations réalisées, exhaustif et officiel.

### Protection des comptes et droits d’accès

Le personnel extérieur s’assure de la protection des comptes et droits d’accès qui lui sont confiés. Il veille notamment à la protection des identifiants et authentifiants qui lui sont confiés.

Il est interdit de créer des comptes à privilèges ou des comptes permettant l’accès à des données confidentielles sans avoir obtenu l’accord du RSSI du CHR : **rssi@chr-metz-thionville.fr**

Seuls des comptes nominatifs seront délivrés, le personnel extérieur s’engage à ne pas créer de compte générique y compris pour l’accès à ses applications.

Il ne les utilise que pour les activités et besoins directement liés aux tâches dont il a la charge. En particulier, il veille à ne pas abuser de ses privilèges, et limite ses actions aux ressources informatiques auxquelles il a accès, dans le respect de la finalité de sa mission.

En particulier, il ne modifie les configurations et les droits d’accès que dans le cadre des procédures définies, lorsqu’elles existent.

Pour les accès aux ressources du SI de l’établissement il utilise des mots de passe robustes respectant les recommandations de l’ANSSI.

A savoir au minimum : complexité du mot de passe, 15 caractères et renouvellement au minimum tous les ans.

Le personnel extérieur s’engage à ne pas noter le mot de passe ou tout autre code d’authentification dans un endroit non sûr (ex. post-it à proximité du poste, en clair dans un fichier).

Il s’engage par ailleurs à verrouiller sa session lorsqu’il s’absente de son poste et à ne pas laisser le poste accessible sans surveillance.

### Déclaration des vulnérabilités et incidents

Le personnel extérieur s’engage à remonter sans délai à son correspondant du CHR toute vulnérabilité et tout incident de sécurité qu’il constate ou suspecte, incluant la perte ou le vol de supports informatiques contenant des données du CHR, ou bien la compromission d’un compte d’accès au SI de l’établissement.

### Traçabilité et contrôle

Le CHR se réserve le droit de vérifier, par tout moyen, le bon usage des ressources informatiques et le respect des règles édictées par la présente charte.

L’utilisation des ressources informatiques de l’établissement génère des traces informatiques pouvant contenir des données à caractère personnel des utilisateurs, telles l’adresse IP ou l’identifiant du poste de travail, le login de l’utilisateur, les dates et heures des actions, les ressources accédées et/ou les actions réalisées.

Ces traces peuvent faire l’objet de traitements par l’établissement à des fins statistiques, de maintenance des équipements, de contrôle du respect des règles de sécurité, de respect des droits des patients, de protection du SI et des informations qu’il contient, ou d’enquêtes en cas d’incident ou de suspicion d’incident technique ou de sécurité.

Les traitements réalisés sur ces données respectent les exigences légales et réglementaires.

### Engagement de confidentialité

Je m’engage conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés ainsi qu’aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l’état de l’art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j’ai accès, et en particulier d’empêcher qu’elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

**Je m’engage en particulier à :**

* ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
* ne divulguer ces données qu’aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu’il s’agisse de personnes privées, publiques, physiques ou morales ;
* ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l’exécution de mes fonctions ;
* prendre toutes les mesures conformes aux usages et à l’état de l’art dans le cadre de mes attributions afin d’éviter l’utilisation détournée ou frauduleuse de ces données ;
* prendre toutes précautions conformes aux usages et à l’état de l’art pour préserver la sécurité physique et logique de ces données ;
* m’assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
* en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d’information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu’en soit la cause, dès lors que cet engagement concerne l’utilisation et la communication de données à caractère personnel.

J’ai été informé que toute violation du présent engagement m’expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

## Acte d’engagement personnel

Je soussigné

employé(e) de la société

🞏 Atteste avoir pris connaissance du contenu de la présente charte

🞏 M’engage à respecter les principes, règles, directives énoncées dans la charte

*(Cases à cocher)*

* Activités et objectifs de la mission :
* Périmètre applicatif et/ou technique :
* Interlocuteur(s) CHR :
* Votre numéro de téléphone (portable de préférence afin d’être joignable directement si nécessaire) :
* 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)

Fait à le

Signature