CHARTE DE CYBERSECURITE DU CHU PLAINSBORO A DESTINATION DES SALARIES

Rédaction le 05/10/2025
DPO – Dana Scully

Vérification le 10/10/2025
RSSI – Anaïs Martins
Service juridique – Elle Woods

Approbation le 15/10/2025
Direction – Lisa Cuddy

Date d'application : 20/10/2025

Table des matières

---

1. Objet et champ d'application

La présente charte définit les règles d'accès et d'usage des ressources informatiques et des services numériques du CHU.
Elle a pour but d'assurer la sécurité du système d'information, de protéger les données des patients et du personnel, et de garantir la continuité et la qualité des soins.

Elle s'applique à tous les utilisateurs : agents, stagiaires, internes, prestataires ou tout intervenant ayant accès au réseau, aux équipements ou aux applications du CHU.
Sont concernées toutes les ressources informatiques : ordinateurs, tablettes, téléphones, imprimantes, messageries et connexions à distance.

Risques en cas de cyberattaque

Il est essentiel de comprendre que les menaces numériques ne sont pas théoriques : elles peuvent avoir des conséquences graves sur la prise en charge des patients et le fonctionnement de l'hôpital. Une faille de cybersécurité peut entraîner :

- **L'arrêt ou la réduction d'activité de services médicaux essentiels** (radiologie, laboratoire, bloc opératoire), fortement dépendants des systèmes informatiques ;
- **L'indisponibilité des postes informatiques**, rendant impossible la consultation des dossiers médicaux ou la prescription de traitements ;
- **La paralysie d'équipements médicaux connectés** tels que les IRM, scanners ou dispositifs de monitoring ;
- **L'interruption de la circulation des données patients**, empêchant la continuité des soins entre services.

Ces risques sont réels : en 2020, une cyberattaque en France a entraîné le décès d'une patiente faute d'accès aux soins à temps, illustrant l'impact direct de la cybersécurité sur la vie humaine.

2. Principes fondamentaux de la sécurité

Le CHU gère des informations sensibles : dossiers médicaux, données administratives, informations internes.
Ces données doivent être protégées selon quatre critères essentiels :

- **Confidentialité** : seules les personnes autorisées y accèdent.
- **Intégrité** : les données doivent rester exactes et complètes.
- **Disponibilité** : les informations doivent être accessibles quand nécessaire.
- **Traçabilité** : chaque action doit pouvoir être identifiée.

La sécurité repose autant sur les outils techniques que sur le comportement responsable de chaque utilisateur. Une seule négligence peut compromettre la sécurité de tout le système.

3. Règles de sécurité et bonnes pratiques

Comptes et mots de passe

Chaque utilisateur dispose d'un compte personnel (login, mot de passe).
Le mot de passe doit être **personnel, robuste et renouvelé régulièrement**. Il ne doit jamais être partagé.
Il est obligatoire de **verrouiller sa session** en cas d'absence et de **fermer sa session** avant de quitter son poste.

Confidentialité et discrétion

Le personnel est soumis au **secret professionnel et médical**.
Aucune donnée de santé ne doit être communiquée sans autorisation ni transmise via une messagerie non sécurisée.
Pour limiter ce risque, la diffusion de contenu lié au CHU est interdite sur les réseaux sociaux du personnel (informations écrites ou photos).
L'accès aux informations est limité aux seules données nécessaires à la mission de l'utilisateur.

Matériel et stockage

Aucune donnée sensible ne doit être enregistrée sur un poste local, une clé USB ou un support personnel.
Ne branchez jamais sur votre équipement informatique une clé USB trouvée ou donnée par un patient. Utilisez uniquement **les clés USB fournies** par le CHU.
Les documents doivent être stockés sur les serveurs sécurisés du CHU.
Tout matériel (ordinateur, tablette, dossier papier) doit être **rangé et verrouillé** lorsqu'il n'est pas utilisé.

Messagerie et Internet

- N'ouvrez **aucun lien ou pièce jointe suspecte**.
- Ne répondez jamais à un **e-mail suspect**.
- L'usage d'Internet et de la messagerie doit rester **strictement professionnel**.
- Les échanges de données médicales ne doivent se faire que via les outils **sécurisés** du CHU.

Séparation des usages personnels et professionnels

Les équipements du CHU sont destinés à un usage **professionnel**.
L'usage d'équipements personnels n'est permis qu'en cas d'autorisation spécifique du service informatique.

4. Protection des données et conformité réglementaire

Le CHU respecte la réglementation en vigueur : RGPD, secret médical, loi Informatique et Libertés.
Toute collecte ou traitement de données personnelles doit être validé par la Responsable de la Sécurité du Système d'Information (RSSI) ou le Délégué à la Protection des Données (DPO).
Le non-respect de ces règles peut entraîner des sanctions pénales.

Les utilisateurs doivent signaler immédiatement toute **anomalie, perte de données ou suspicion d'incident** de sécurité.

En cas de doute, contactez immédiatement le service informatique :

- E-mail : securite-si@chu-plainsboro.fr

- Tél : 05.11.12.13.14

Signaler, ce n'est pas déranger, c'est protéger.

5. Traçabilité, surveillance et responsabilités

L'établissement met en place des outils de **traçabilité** pour enregistrer les connexions, opérations et accès aux données.
Ces informations sont confidentielles mais peuvent être consultées en cas d'enquête ou d'incident.

Chaque utilisateur est responsable de l'usage fait de son compte et de son matériel.
Tout manquement à la présente charte peut entraîner des sanctions disciplinaires, telles qu'un avertissement, un retrait d'accès, voire des poursuites civiles ou pénales en cas de faute grave.

Fait à Toulouse, le 20/10/2025

Lisa CUDDY – Directrice du CHU
Anaïs MARTINS - RSSI – Responsable de la Sécurité du Système d'Information
Dana Scully - DPO – Déléguée à la Protection des Données
Elle Woods – Service juridique

Engagement des utilisateurs

En signant cette charte, chaque utilisateur s'engage à :

- **Respecter** l'ensemble des règles énoncées

- **Protéger** les données dont il a la responsabilité

- **Signaler** tout incident ou suspicion d'incident

- Utiliser les ressources informatiques de manière **responsable**

Je reconnais avoir pris connaissance de cette charte et m'engage à la respecter.

Date et signature