


|   |   |                             |
|---|---|-----------------------------|
| <br>Hôpitaux de Toulouse | Politique de sécurité de l'information  | Version 2.0<br>20 août 2019 |
|   | Charte d'utilisation du Système d'Information à destination des titulaires de profils à pouvoir |                             |

## 1 Rappel du contexte de la Charte d'utilisation du Système d'Information à destination des titulaires de profils à pouvoir

Dans le cadre de leurs missions, les Hôpitaux de Toulouse configurent, administrent, supervisent, maintiennent et exploitent les infrastructures (réseaux, serveurs, bases de données, ...) et les postes de travail de son Système d'Information.

Les usages et pratiques en relation avec ces activités nécessitent de disposer, pour des intervenants identifiés, de profils utilisateurs particuliers fournissant des droits d'accès et d'actions étendus.

Les droits d'accès visés concernent notamment :

- le contrôle et la modification de données physiques ou numériques stratégiques ou privatives pour l'établissement,
- les données de configuration.

La responsabilité des titulaires de profils à pouvoir et, à travers eux, des personnes impliquées, exigent le respect d'un cadre précis garantissant au mieux l'intégrité, la disponibilité, la confidentialité et la traçabilité des informations.


Toute demande de création, modification ou suppression d'accès à pouvoir sera réalisée par le responsable CHU31 du titulaire au travers d'un outil institutionnel adapté (C4U) afin d'assurer la traçabilité de cette demande et le respect des procédures en vigueur.

Les droits d'administration et de gestion dont disposent les profils à pouvoir constituent le niveau le plus élevé dans la hiérarchie des accès aux informations de l'établissement (CHU de Toulouse)

Les responsabilités qui en résultent doivent déterminer un fort niveau d'engagement en termes de confiance et de responsabilité.

Cet engagement est matérialisé par la signature de la présente charte, spécifiquement dédiée aux titulaires de profils à pouvoir.

En cas de manquement aux obligations consignées dans la présente charte, le CHU Toulouse est susceptible d'engager toute mesure disciplinaire ou légale appropriée à l'encontre du titulaire du / des profils à pouvoir.

|   |   |                             |
|---|---|-----------------------------|
|  | Politique de sécurité de l'information  | Version 2.0<br>20 août 2019 |
|   | Charte d'utilisation du Système d'Information à destination des titulaires de profils à pouvoir |                             |


## 2 Charte d'utilisation du Système d'Information à destination des titulaires de profils à pouvoir

Le titulaire de profils à pouvoir et des droits associés (ci-après nommé « le titulaire ») contribue à l'usage correct des biens et informations en respectant les principes suivants :


1. La présente charte s'applique à tout titulaire (agents, personnels temporaires, partenaires, fournisseurs...).
2. Le titulaire doit se conformer aux règles et procédures mises en œuvre par l'établissement pour assurer la gestion et la sécurisation de l'information, notamment la PSSI du CHU de Toulouse et la PSSI couvrant le périmètre ISO27001 au CHU Toulouse.
3. Le titulaire doit respecter l'intégrité des moyens qui lui sont confiés dans le respect des usages affectés, sans perturber leur fonctionnement et sans y apporter de modifications directes ou indirectes.
4. Tous les attributs de connexion et droits fournis au titulaire sont strictement personnels et inaccessibles.

Chaque titulaire est donc responsable et s'engage:

- à ne pas communiquer ses identifiants et/ou mots de passe et à les changer régulièrement (changement souhaité tous les 90 jours)
  - à signaler immédiatement auprès de son encadrement toute perte, vol, destruction ainsi que toute tentative de violation de son compte et, de manière générale, toute anomalie qu'il pourrait constater.
  - à ne pas réutiliser ses mots de passe (profils à pouvoir) à d'autres fins et/ou usages (sites ou applications)
5. L'ensemble des moyens et des droits fournis au titulaire sont mis à disposition dans le cadre unique des activités de l'établissement (CHU de Toulouse).
  6. Le titulaire de profil à pouvoir est responsable des données qu'il consulte, télécharge, utilise, transfère ou diffuse.
  7. Le titulaire de profil à pouvoir reconnaît avoir reçu toutes les informations nécessaires liées aux moyens mis en œuvre pour sécuriser les technologies de l'information au sein de l'établissement (CHU de Toulouse).

|   |  |   |
|---|--|---|
| <br>Hôpitaux de Toulouse | <b>Politique de sécurité de l'information</b>  | <b>Version 2.0</b><br><b>20 août 2019</b> |
|   | <b>Charte d'utilisation du Système d'Information à destination des titulaires de profils à pouvoir</b> |   |

8. Le titulaire de profils à pouvoir doit veiller sur le matériel informatique qui lui est confié et notamment :
  - ne jamais laisser le(s) poste(s) de travail sans surveillance,
  - ne pas entraver le fonctionnement des systèmes de sécurisation.
  
9. L'utilisation des profils à pouvoir fournis est subordonnée à un comportement non répréhensible dans le respect des lois et réglementations et, notamment, sur les aspects relatifs :
  - au respect de la vie privée et de la protection des données à caractère personnel et des données médicales,
  - à la protection de la propriété intellectuelle (protection des logiciels, protection des bases de données, propriété littéraire et artistique),
  - à la lutte contre la fraude informatique,
  - à la loi « Informatique et libertés » et du RGPD,
  - à la cryptologie,
  - au secret des correspondances et à l'interdiction d'interception des communications émises par voie des télécommunications.
  
10. Dans le cadre de ses missions, le titulaire de profil à pouvoir peut être amené :
  - à gérer les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements qui pourraient d'une part constituer un incident de sécurité, et/ou d'autre part faire l'objet d'une réquisition émise par les autorités judiciaires,
  - à conduire cette journalisation en garantissant le respect des lois et des règlements, en particulier ceux relatifs à la protection des données personnelles et au secret des correspondances privées,
  - à constater des anomalies de fonctionnement ne relevant manifestement pas de problèmes techniques - le titulaire de profil à pouvoir doit aussitôt rendre compte de ces anomalies à son encadrement.

|   |   |                             |
|---|---|-----------------------------|
|  | Politique de sécurité de l'information  | Version 2.0<br>20 août 2019 |
|   | Charte d'utilisation du Système d'Information à destination des titulaires de profils à pouvoir |                             |

11. L'utilisateur de profils à pouvoir est soumis au devoir de secret professionnel qui découle de sa fonction :

- il s'engage à observer le secret professionnel pour tout ce qui concerne l'exercice de ses fonctions et, d'une façon générale, pour tout ce dont il a eu connaissance directe ou indirecte dans l'exercice de sa fonction,
- il ne peut à ce titre déléguer aucune partie de ses droits ou de ses missions et est responsable de ses actions,
- il ne peut en aucun cas modifier les droits attribués aux utilisateurs ou à d'autres titulaires dont les droits sont inférieurs aux siens en dehors des procédures prévues à cet effet,
- il ne peut pas accéder aux informations personnelles,
- Tous types de documents, même rédigés par lui, reste la propriété de l'établissement (CHU de Toulouse).
- Il reste soumis à ses obligations de confidentialité même après la fin de son contrat (continuité des engagements) avec le CHU de Toulouse.

#### Signature d'engagement du titulaire de profils à pouvoir

Je soussigné(e) :

Grade/fonction :

Etablissement/Société :

Service :

Déclare avoir pris connaissance et accepter de respecter la présente charte d'utilisation du Système d'Information en tant que titulaire de profils à pouvoir

Date

Signature