FICHE RÉFLEXE

SÉCURISATION DES POSTES DE TRAVAIL

Les postes de travail servent d'interface vers le Dossier Patient Informatisé (DPI) et d'autres applications critiques.

#1 ACCÈS RESTREINT DU POSTE DE TRAVAIL

- **Authentification par carte à puce** (carte nominative CPS/CPE)

> La carte CPE/CPS vous est affectée nominativement dès votre arrivée au sein de l'établissement. Elle vous permet d'accéder à l'établissement, et de vous identifier sur un poste de travail professionnel. Pour s'authentifier, un code PIN doit être saisi à l'écran de verrouillage afin d'accéder à votre session de travail. Ce code ne doit jamais être transmis, ou être affiché en évidence sur votre bureau. En cas de perte, contactez le service RH dè que possible afin d'éviter une utilisation frauduleuse.

- Toujours **verrouiller sa session lorsque l'on quitte son poste de travail,** soit en utilisant le raccourci Windows : Win + L /, en retirant sa carte CPE/S du boitier de carte, ou Ctrl+Alt+Suppr et « Verrouiller ».
- Instaurer la **mise en veille automatique** au bout de quelques minutes d'inactivité.
- Chaque professionnel doit utiliser ses propres accès. **Pas de session « partagée pour tout un service ».**
- **Déconnecter et éteindre les appareils** non utilisés pour éviter un accès distanciel malveillant, ou en fin de journée avant de quitter votre bureau

#2 MISES À JOUR LOGICIEL

- Pensez à **appliquer les mises à jour** immédiatement dès qu'une notification système apparait (dans notre cas Windows).
- Redémarrez votre poste pour **appliquer les correctifs** avant de terminer votre journée.
- Une maintenance des applications métiers est régulièrement planifiée afin de pouvoir effectuer les mises à jour. Une note de service est communiquée à cet effet.
- Éviter de reporter une mise à jour système sous prétexte qu'elle prend trop de temps.

#3 LIMITATION DE L'INSTALLATION DE LOGICIELS

- **Demander obligatoirement l'avis du service informatique** sur un logiciel avant son installation.
- **Vérifiez** régulièrement **la liste des programmes** installés.

#4 STOCKAGE DES DOCUMENTS

- **Supprimer les fichiers sensibles** de votre poste une fois utilisés, et vider la corbeille !
- Effectuez les **sauvegardes de documents sur les lecteurs réseaux** (partages sécurisés) attitrés à cet effet.

SIGNALEZ IMMÉDIATEMENT

- Une personne inconnue qui aurait effectuée des actions suspectes sur un poste déverrouillé.
- Des comportements étranges (logiciel inconnu, curseur qui bouge seul)

Avertir le service informatique
1017 ou 05 55 43 10 17

Ou nous contacter sur
informatique@ch-esquirol-limoges.fr