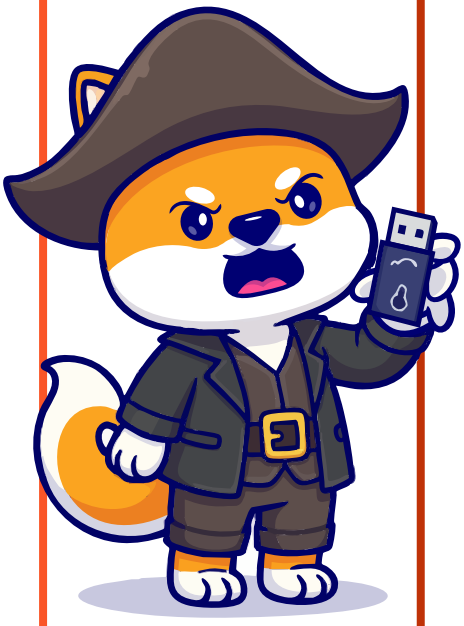
FICHE RÉFLEXE

UTILISATION SÉCURISÉE DES CLÉS USB ET SUPPORTS AMOVIBLES



Les clés USB, les disques durs externes, ou encore les smartphones sont simples à égarer, et un tiers peut y accéder s'il n'y a pas de chiffrement ou un mot de passé sécurisé.

Au sein de notre hôpital, ces supports peuvent contenir des rapports très confidentiels (audio d'entretiens, images...).

#1

UTILISER UNIQUEMENT DES SUPPORTS DE SOURCE SÛRE

- Clés USB, disques durs externes chiffrés et approuvés par le service informatique (Procédé pour demande support amovible dans un contexte professionnel)
- Éviter d'acheter et de brancher des supports inconnus.
- Si support non reconnu, ne pas insister et ne pas reformater sans avis de la DSI

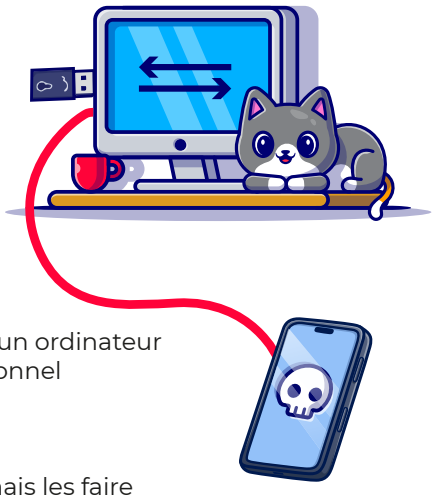
#2

RANGER LES SUPPORTS EN LIEU SÛR

- Dans un tiroir ou une armoire fermée à clé.
- Éviter de les laisser branchés inutilement sur un poste.

#3

- Ne jamais prêter ses supports, et veiller à ce qu'ils ne quittent jamais l'hôpital



#4

- Eviter de transférer des données sensibles sur un périphérique externe personnel

#5

- Éviter d'utiliser un périphérique externe sur un ordinateur personnel puis sur votre ordinateur professionnel

#6

- En ce qui concerne les smartphones, ne jamais les faire recharger sur votre ordinateur personnel, car vecteur de virus: toujours privilégier le rechargement par secteur

EXEMPLE CONCRET

Cas pratique : Vous devez transférer des photos cliniques. Vous utilisez une clé USB dédiée, chiffrée, validée par la DSI. Vous évitez d'utiliser la clé USB personnelle que vous avez dans votre sac.

SIGNALEZ IMMÉDIATEMENT

- Si vous trouvez une clé USB « abandonnée » dans un couloir ou un bureau.
- En cas de perte ou vol d'une clé USB contenant des informations.

Avertir le service informatique
1017 ou 05 55 43 10 17

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

Nous rapporter le support amovible inconnu pour analyse