



NOTE D'INFORMATION

A l'attention des professionnels équipés d'un poste informatique attitré

L'Isle-Adam, le 22/10/2024

Service : qualité / SIH

Tel : 01 34 69 76 63

Réf : FH

Objet : sécurisation du stockage des mots de passe professionnels

Madame, Monsieur,

Afin d'assurer la sécurité du stockage des mots de passe que vous utilisez dans le cadre de votre activité professionnelle au sein de l'établissement ;

→ vous êtes tenus d'enregistrer vos mots de passe (ainsi que vos identifiants et URL de connexion) **exclusivement** sur le gestionnaire de mots de passe sécurisé dénommé KEEPASS.

L'enregistrement sur fichier Word ou Excel, même si vous soumettez l'ouverture du fichier à un mot de passe, est interdit. L'enregistrement sur papier l'est également.

Le gestionnaire de mots de passe KEEPASS est disponible pour tous les professionnels.

Les professionnels qui ne l'ont pas encore mis en place doivent contacter au plus vite :

- Florine Herbillon au 76 63 / qualite@hgiap.fr
- Guillaume Chammah au 70 33 / stage@hgiap.fr
- Emilie Saint Germain au 70 31 / aqualite@hgiap.fr
- Ou faire un ticket informatique sur BK

Afin de mettre en place KEEPASS le plus rapidement possible.

Les bases de données KEEPASS sont toutes enregistrées dans le dossier partagé nommé KEEPASS disponible sur le réseau ECHANGE.

Attention, vous êtes le seul à connaître votre mot de passe maître permettant d'ouvrir votre base de données KEEPASS : ne l'oubliez pas !

La procédure ADM7-PR-012 « Stockage des bases de données et des mots de passe maîtres KEEPASS dans le cadre du Plan de Continuité et de Reprise d'Activités » est disponible en GED. Elle explique comment les bases de données KEEPASS sont sauvegardées.



Voici une brève description de l'Outil KEEPASS :

Il s'agit d'un gestionnaire de mots de passe open-source, conçu pour stocker et gérer de manière sécurisée des mots de passe et d'autres informations sensibles.

Ses principales caractéristiques sont :

- Stockage sécurisé : KeePass conserve les mots de passe dans une base de données chiffrée à l'aide d'algorithmes robustes comme AES-256 ou ChaCha20. Cela protège les données contre les accès non autorisés.
- Accès par mot de passe principal : Pour accéder à la base de données, l'utilisateur doit entrer un "mot de passe principal", qui est la seule information à mémoriser. Une clé de fichier ou une combinaison des deux peut également être utilisée pour un niveau de sécurité supplémentaire.
- Organisation des mots de passe : Les utilisateurs peuvent organiser leurs mots de passe en catégories ou dossiers, ajouter des notes, URL, et personnaliser les champs pour chaque entrée.
- Générateur de mots de passe : KeePass dispose d'un générateur de mots de passe intégré qui crée des mots de passe forts et aléatoires pour chaque compte.
- Portabilité : Le logiciel est portable, ce qui signifie qu'il peut être utilisé directement à partir d'une clé USB sans nécessiter d'installation sur l'ordinateur hôte.
- Extensions et plugins : KeePass prend en charge des extensions et des plugins développés par la communauté pour ajouter de nouvelles fonctionnalités ou améliorer son intégration avec d'autres logiciels.
- Multiplateforme : Bien que KeePass soit principalement conçu pour Windows, des versions compatibles existent pour Linux, macOS, Android, iOS, et d'autres plateformes via des ports ou des applications tierces.

Les établissements de santé étant particulièrement exposés à la menace de cyber attaque, nous devons sécuriser au maximum notre système d'information hospitalier et les données de nos patients. L'utilisation d'un gestionnaire de mots de passe sécurisé est ainsi indispensable.

Je vous remercie par avance pour l'attention que vous porterez à cette note d'information et vous prie de recevoir, Madame, Monsieur, mes salutations les plus sincères.

Florine HERBILLON
RSSI