# RGPD
# Les 10 bonnes pratiques de protection informatique

## ① MOTS DE PASSE

Les mots de passe sont les premiers codes d'authentification permettant l'accès à vos données personnelles et/ou publiques. Ils ouvrent l'accès à vos messageries, réseaux, outils de gestion, …

De ce fait, ils doivent être difficilement accessibles par un tiers.

- ⇨ Choisir des mots de passe différents comportant des majuscules, minuscules, chiffres et caractères spéciaux ;
- ⇨ les changer régulièrement par trimestre ou semestre par exemple ;
- ⇨ Ne pas les communiquer.
- ⇨ Mettre en place un verrouillage automatique du PC après une durée limitée d'inactivité.

Accès interdit au poste d'un collègue absent sauf dispositions spécifiques prévues à cet effet.

## ② UTILISATION DE LA MESSAGERIE

En tant que destinataire :

- ⇨ Identifier les expéditeurs avant d'ouvrir les messages ;
- ⇨ Vérifier les liens des corps de message et les pièces jointes avant de les ouvrir ;
- ⇨ Ne pas utiliser d'adresse personnelle ;
- ⇨ Signaler un courrier indésirable.

En tant qu'expéditeur :

N'envoyez aucune donnée sensible par courriel.

## ③ ACCÈS INTERNET

- ⇨ N'accéder si possible qu'à des sites sécurisés : http**s**//… ;
- ⇨ Limiter la consultation de sites dans un but purement personnel ;
- ⇨ S'assurer des droits avant toute réutilisation : droit d'auteur, de propriété, d'image, plagiat….

## ④ EQUIPEMENT MOBILE (portables, tablettes, téléphones, …)

- ⇨ Ne pas les laisser à la portée de tous ;
- ⇨ Les protéger d'un verrouillage (code d'accès).

## ⑤ SUPPORT AMOVIBLE (disque dur, clé USB, carte mémoire, ...)

Les supports externes (clé USB, etc.) peuvent être infectés et compromettre le bon fonctionnement de votre poste de travail. Ils sont vecteurs de nombreux piratages.

- ⇨ Ne les utiliser que s'ils proviennent d'une source sure.

## ⑥ OUTILS DE PROTECTION

- ⇨ Activer le pare feu ;
- ⇨ Utiliser un antivirus ET veiller à sa mise à jour régulière ;
- ⇨ Ne pas désactiver les paramétrages de sécurité.

## ⑦ SAUVEGARDE

- ⇨ Sauvegarder régulièrement vos documents ;
- ⇨ Les stocker sur les espaces réservés à cet effet (serveur, disque dur externe, etc.).

En cas de sauvegarde via un outil externe, sécuriser le lieu d'accès à celui-ci pour le protéger du vol et permettre la récupération de vos données.

## ⑧ ORDINATEUR INFECTE

- ⇨ Débrancher votre unité centrale ;
- ⇨ Prévenir sans tarder votre correspondant informatique ;
- ⇨ Changer vos mots de passe via un autre poste.

## ⑨ CONSCIENCE / CONFIDENTIALITE

La sécurité n'est pas que technique, elle passe par l'utilisation que vous faites des outils mis à votre disposition.

Respecter l'obligation de confidentialité des informations professionnelles dont vous avez connaissance dans le cadre de votre service (maintenance, administrateur, …)

## ⑩ CONFORMITE

Mettre en place une charte informatique et la respecter.

⚠ En cas d'absence ou de départ d'un agent prévoir les modalités de consultation, restitution, suppression, … des accès qu'il détient.