



## 1. ÊTRE RESPECTUEUX DU MATÉRIEL

Ne pas déplacer un PC fixe en fonctionnement.

Ne pas éteindre un PC avec le bouton marche arrêt mais bien passer par le menu.

Ne pas manger ni boire sur son pc.

## 2. PROTÉGER SON POSTE DE TRAVAIL ET SES DOCUMENTS

Vous ne devez pas laisser :

Votre pc ouvert.

Vos applications sensibles doivent être fermées lorsque vous avez terminé de travailler.

Vous devez verrouiller votre PC lorsque vous quittez votre bureau.

Vous devez fermer la porte de votre bureau en votre absence et ne pas oublier de verrouiller votre PC.

Une personne brancher une clé USB à votre PC lors d'une réunion sans l'avoir tester avec votre antivirus avant

Mettez des mots de passe sur vos documents sensibles.

## 3. AVERTIR L'INFORMATIQUE SI

Problème de PC, Virus , Ransomware ou en cas de suspicion.

## 4. DIALOGUER AVEC L'INFORMATIQUE

Les services techniques peuvent prendre la main à distance sur votre poste, pour cela n'acceptez que les utilisateurs avec qui vous êtes en contact téléphoniques et que vous avez appelé ou que vous pouvez identifier.

En règle générale, ces prises de contrôles se font avec Landesk(APF) , Logme In (APF), Teamwiever (Gesper, Waysoft) et Zoho Assist (Gosoins).

Ne pas donner la main si vous n'êtes pas informé d'un problème !

## 5. STOCKER CE QUI EST UTILE ET NÉCESSAIRE

Ne soyez pas un stockeur compulsif : Tout enregistrer dans mes documents sans classer et Télécharger, tout et toujours, est inutile et surcharge votre PC.

Cela vous ralentit dans votre quotidien lors de vos recherches urgentes. Trier et faire le ménage régulièrement vous permettra une gestion saine de vos documents.

## 6. ORDONNER LES DOCUMENTS

Respecter le plan de nommage qui vous a été communiqué. Une fiche "Plan de nommage" est disponible sur Bluemedi si vous avez un doute.  
Trier et faire le ménage régulièrement vous permettra une gestion saine de vos documents.

## 7. NAVIGUER AVEC ATTENTION SUR LE WEB

N'utilisez pas Internet Explorer, restez avec Firefox et Google Chrome  
Vérifier la ligne en vert des liens internet lors d'une recherche Google.  
Téléchargez les programmes sur les sites officiels des éditeurs, "ne faites pas une recherche Google en cliquant sur la première réponse donnée ,vous allez devoir payer ou vous faire pirater dans 3 cas sur 4 !  
Être vigilant lors d'un paiement sur Internet, le site doit être https  
Essayez de ne pas conserver vos historiques de navigation internet trop longtemps.

## 8. GÉRER VOTRE BOITE MAIL

Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire).  
Des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing »\*

Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus\* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

Ne répondez pas à tout le monde

## 9. SOYEZ VIGILANTS

Se connecter à des sites depuis sa boîte mail vous indiquant que vous devez payer une facture, que la caf va vous faire un cadeau de 500 euro ou que votre ligne téléphonique va être coupée  
Les banques communiquent par téléphone ou par courrier, la caf fait rarement de cadeau, et votre opérateur vous enverra un sms pour vous indiquer que votre facture est impayée ou votre compte bloqué.

Ne cliquez surtout pas directement depuis le mail, choisissez d'aller sur le site manuellement de votre opérateur ou du fournisseur, et connectez-vous à votre espace client et vérifiez vos messages .

## 10. DIFFÉRENCIER PROFESSIONNEL ET PERSONNEL

### 11. LES RÉSEAUX SOCIAUX

N'utilisez pas les réseaux sociaux sur votre poste de travail professionnel ou autres sites et forums à usage personnel !

### 12. RESPECTER LE RGPD (CNIL)

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.  
Respecter la confidentialité des données de vos usagers.

Ne pas utiliser ou créer des tableaux avec des données sensibles qui ne sont pas utiles !  
Je n'ai pas besoin du numéro de SS pour faire un tableau d'animation ...

### 13. LES APPAREILS MOBILES à LA MAISON

Vous et vous seul êtes autorisés à l'usage des appareils mobiles remis par votre employeur.  
Vos conjoints, enfants, ne peuvent en aucun cas utiliser ces appareils.

### 14. ÊTRE MOBILE AVEC SON MATÉRIEL

Attention lors des transports en voiture : ne pas laisser le portable sur le siège arrière et la voiture non fermée en roulant notamment dans les bouchons.  
Transport dans les transports en commun : utilisez des cartables neutres et non ostentatoire.  
Utilisez que des clés U3 cryptées avec mot de passe si la clé contient des données de vos usagers.

Déconnecter le wifi et le Bluetooth en partant du bureau.

Ne vous connectez pas à des réseaux wifi gratuit avec votre pc entreprise ou votre smartphone !  
Même à titre particulier, en acceptant la connexion vous partagerez vos photos ou toutes autres informations confidentielles inscrites dans votre smartphone et vous mettez en péril la sécurité personnelle de vos proches et celle de votre société !

N'utilisez pas les wifi des hôtels avec un PC de travail, préférez une connexion en 4G avec votre smartphone !

### 15. EN CAS DE DOUTE, FAITES VOUS ASSISTER

Quel que soit le doute ou la question, interrogez votre partenaire informatique, votre direction, votre responsable informatique, votre correspondant DPO.  
Ayez un avis clair et précis et évitez ainsi les erreurs.

**Une question n'est jamais bête, ne pas le poser peut l'être :)**

