

# COVID 19 - Protection de l'information

## Que faut-il protéger ?

## Que faut-il protéger ?

**L'ENSEMBLE DES INFORMATIONS MANIPULEES** : création, réception, traitement, destruction

La mauvaise utilisation ou la divulgation des informations traitées dans le cadre du COVID-19 peut porter gravement atteinte à la gestion de la crise sanitaire et fragiliser la réponse gouvernementale pour faire face à la pandémie.

Cette protection de l'information engage notre responsabilité individuelle et collective ; il appartient donc à tous de mettre en œuvre les moyens de protection pour réduire les vulnérabilités.

## Comment protéger ?

## Comment protéger ?

### 1. ASSURER LA SÉCURITÉ PHYSIQUE : Protection des locaux

- ✓ port obligatoire du badge ;
- ✓ demander à toute personne inconnue dans les locaux de se présenter et de justifier sa présence ;
- ✓ restriction d'accès à certaines salles réglementées et interdites à toute personne non autorisée ;
- ✓ restriction d'accès aux réunions « sensibles » et fermeture des accès pendant les réunions.

#### ➤ Visiteurs :

- ✓ établir un registre des visites : identité, heures d'arrivée et de départ, objet de la visite ;
- ✓ faire accompagner le (s) visiteur (s) durant leurs déplacements dans les locaux ;
- ✓ être attentif et conserver une certaine réserve dans les propos échangés avec les visiteurs.

### 2. PROTÉGER L'INFORMATION : Comportements à adopter au quotidien

#### ➤ Documents – Informations considérés comme « sensibles » :

- ✓ production : marquer les documents avec les mentions « Diffusion Restreinte » ou « Diffusion Limitée » (niveau de marquage à l'approbation de l'autorité) ;
- ✓ ranger les documents sensibles sous clé : pause déjeuner, fin d'activité, nettoyage des bureaux,... ;
- ✓ lors des relèves d'équipes ou de poste, passage de consignes sur les sujets et/ou documents sensibles ;
- ✓ détruire les documents devenus inutiles, y compris les brouillons : utilisation systématique de destructeurs ;
- ✓ chrono et/ou archives : à stocker dans des armoires fermées à clé.

#### ➤ Numérique

- ✓ stocker les informations COVID-19 sur un répertoire spécifique et protégé ;
- ✓ ne pas laisser son login - mot de passe accessible sur son poste de travail ;
- ✓ verrouiller sa session dès que l'on s'éloigne de son ordinateur ;
- ✓ utiliser des supports informatiques dont la provenance est connue ;
- ✓ protéger son ordinateur portable dans les transports publics et à son domicile ;
- ✓ rendre compte de tout incident et faire appel à une personne ressource qualifiée (RSSI).

#### ➤ Réunions :

- ✓ participation aux réunions : s'assurer de l'identité des participants ;
- ✓ après toute réunion : récupérer les documents, effacer les tableaux et retirer les feuilles des paperboards ;
- ✓ audioconférences : - changer régulièrement les codes d'accès ;  
- ne pas aborder les informations les plus sensibles.

#### ➤ Echanges professionnels

- ✓ ne pas communiquer sur les actions en cours sans validation formelle des autorités ;
- ✓ s'assurer de l'identité des nouveaux correspondants ;
- ✓ ne transmettre les informations que l'on traite qu'aux personnes autorisées (**le besoin d'en connaître**) ;
- ✓ mettre à jour régulièrement les listes de destinataires.

#### ➤ Echanges et communication ne relevant pas du domaine professionnel

- ✓ respect impératif du devoir de réserve qui s'impose à tout agent public ou collaborateur occasionnel :
  - avec les collègues dans les lieux de vie : restaurant administratif, espace fumeurs... ;
  - avec ses proches ;
  - dans son activité sur les réseaux sociaux ;
- ✓ signaler à son responsable hiérarchique les tentatives d'approche pour obtenir des informations : messages, appels téléphoniques, SMS, réseaux sociaux... (conserver les preuves).

Pour toutes demandes d'informations relatives à la protection de l'information ou des données, contactez :

[hfds@sg.social.gouv.fr](mailto:hfds@sg.social.gouv.fr)