Directive du Bureau du Chef de l'Information : TI 13.08	Publié : 04/2019
Chapitre : Responsabilités des utilisateurs Objet : Ordinateurs portables	Dernière révision : 01/2024

1 DIRECTIVES

1.01 Ceux qui utilisent un ordinateur portable appartenant à l'organisation hors des locaux de l'organisation ou qui stockent des données sensibles de l'organisation sur l'ordinateur doivent prendre les mesures de sécurité décrites dans les procédures de la présente directive.

1.02 Si des données sensibles de l'organisation sur l'ordinateur portable doivent être récupérées hors site, l'utilisateur doit obtenir l'autorisation du gestionnaire pour utiliser et transporter ces données hors site.

2 OBJET

2.01 La présente directive a pour objet de réduire au minimum les risques pour la sécurité des ordinateurs portables appartenant à l'organisation et des données sensibles de l'organisation lorsque les ordinateurs se trouvent à la fois dans les locaux de l'organisation et à l'extérieur.

3 PORTÉE

3.01 La présente directive s'applique à tous les utilisateurs autorisés à utiliser et à transporter les ordinateurs portables appartenant à l'organisation.

4 RESPONSABILITÉ

4.01 **Tous les utilisateurs** doivent suivre les processus ou procédures fournis par l'organisation et consignés pour utiliser et transporter les ordinateurs portables appartenant à l'organisation afin de les protéger contre la perte et de protéger les données, les systèmes informatiques et les réseaux de l'organisation contre les risques liés à l'utilisation, au transport, à la réaffectation et à la mise hors service de ces ordinateurs.

4.02 Le **service de soutien technique de la TI** doit :

a) Fournir des procédures qui permettent de mettre à jour en tout temps les ordinateurs portables appartenant à l'organisation en ce qui concerne la protection antivirus et la protection par pare-feu s'ils sont connectés hors des locaux de l'organisation à des réseaux publics ou autres que ceux de l'organisation au moyen de câbles ou de réseaux sans fil.

b) Déterminer quels mécanismes de cryptage des données et de protection par mot de passe sont appropriés pour protéger les données sensibles de l'organisation sur les ordinateurs portables hors site et fournir les outils nécessaires pour permettre le cryptage.

c) Supprimer efficacement toutes les données sensibles de l'organisation stockées sur les ordinateurs personnels avant la réaffectation ou la mise hors service des ordinateurs.

4.03 Les **gestionnaires/superviseurs/chefs d'équipe** sont chargés d'évaluer les besoins informatiques hors site de leurs employés et de les autoriser à utiliser et à transporter un ordinateur personnel appartenant à l'organisation à l'extérieur des locaux de l'organisation.

5 DÉFINITIONS

5.01 Un « **ordinateur portable** » est un appareil informatique autonome qui peut être transporté manuellement et fournir l'accès aux données stockées sur l'appareil, le soutien d'une application stockée pour examiner et mettre à jour les données, et avoir la capacité de connexion à d'autres appareils informatiques pour assurer les communications, le transfert de données ou la capacité de terminal informatique. Il peut s'agir d'appareils sans fil, d'appareils de poche et de tablettes.

6 DIRECTIVES CONNEXES

BCI TI 8.02 – Sécurité des systèmes

BCI TI 8.04 – Confidentialité et protection des renseignements personnels

BCI TI 9.02 – Classification des données

BCI TI 9.03 – Contrôles de l'accès aux données

BCI TI 9.04 – Contrôles de la sécurité des applications

BCI TI 9.06 – Cryptage des données

BCI TI 13.01 – Accès aux systèmes et utilisation acceptable des systèmes

BCI TI 13.03 – Mots de passe

BCI TI 13.07 – Supports amovibles

BCI TI 14.01 – AVEC : Dispositifs et systèmes d'exploitation acceptables

BCI TI 14.02 – AVEC : Accès aux systèmes et utilisation acceptable des systèmes