

1 DIRECTIVE

- 1.01 Les utilisateurs ayant une raison opérationnelle justifiable pour copier des données sur un support amovible et emporter le support hors site doivent obtenir l'autorisation écrite de leur gestionnaire pour utiliser ou transporter le support amovible hors site.
- 1.02 Les seuls supports amovibles qui peuvent être utilisés ou connectés à l'équipement ou aux réseaux de l'organisation sont les supports dont l'utilisation a été approuvée par le service de soutien de la TI et qui ont été achetés par l'organisation ou approuvés pour être transférés à l'organisation.
- 1.03 Les supports amovibles doivent être manipulés, protégés, réaffectés et mis hors service conformément aux instructions de la section *Procédures* ci-dessous.

2 OBJET

- 2.01 La présente directive a pour objet de garantir que, en ce qui concerne l'utilisation de dispositifs de stockage de données amovibles approuvés par l'organisation :
- a) La sécurité et l'intégrité des données sont maintenues.
 - b) Les risques pour la stabilité des systèmes et des réseaux informatiques de l'organisation sont réduits au minimum.
 - c) Le risque d'exposer les données sensibles de l'organisation est réduit au minimum pendant que le support amovible est hors site.

3 PORTÉE

- 3.01 La présente directive s'applique à toutes les personnes autorisées à utiliser les systèmes informatiques de l'organisation.

4 RESPONSABILITÉ

- 4.01 Tous les utilisateurs doivent suivre les processus et procédures consignés de l'organisation concernant les supports amovibles afin 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 supports
- 4.02 Le service de soutien de la TI doit :
- a) Évaluer tous les supports amovibles que l'organisation prévoit utiliser et déterminer lesquels sont approuvés pour être acquis et utilisés sur les

systèmes informatiques de l'organisation.

- b) Déterminer quels mécanismes de cryptage des données et de protection par mot de passe sont appropriés pour protéger les données sur des supports amovibles hors site.
- c) Supprimer efficacement toutes les données stockées sur des supports amovibles avant la réaffectation ou la mise hors service des supports.
- d) Évaluer les outils du système qui contrôlent ou consignent la connexion, le retrait et l'utilisation des supports amovibles.

4.03 Les Opérations de la TI sont responsables de surveiller les journaux de connexion/déconnexion des supports amovibles si ceux-ci sont installés.

5 DÉFINITIONS

5.01 Les « **supports amovibles** » comprennent tous les dispositifs et supports de données sur lesquels des données peuvent être écrites et qui peuvent ensuite être facilement retirées de l'ordinateur hôte, conférant ainsi une portabilité aux données qui s'y trouvent. Cette définition s'applique aux dispositifs suivants :

- Disques optiques (CD/DVD et Blu-ray)
- Disque magnéto-optique
- Cartouches de bande
- Lecteurs de cartouches (Jaz, SuperDisk et ZIP)
- Dispositifs de mémoire flash (clés USB) et cartes SD et dispositifs similaires
- Dispositifs de données connectables par clé USB, y compris :
 - Disques durs
 - Lecteurs audio et vidéo numériques (iPod, MP3)
 - Appareils photo numériques
 - Téléphones intelligents et autres téléphones cellulaires
 - Ordinateurs de poche et assistants numériques personnels (PDA)
 - Cadres d'images numériques

6 RÉFÉRENCES et ÉNONCÉS de DIRECTIVE et de PROCÉDURE 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 14.01 – AVEC : Dispositifs et systèmes d'exploitation acceptables

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