Directive du Bureau du Chef de l'Information : TI 9.06	Diffusée : 04/2019
Chapitre : Sécurité des données	Dernière révision : 01/2022
Objet : **Chiffrement des données**	

1 DIRECTIVE

1.01 Des outils de chiffrement des données doivent être disponibles au besoin pour veiller à la protection des données sensibles. Ces outils doivent être envisagés dans les circonstances suivantes :

a) Les données sont stockées sur un ordinateur partagé ou non sécurisé;

b) Les données sont transmises dans un milieu hostile. Les supports amovibles contenant des données sensibles transportés physiquement à l'extérieur de l'organisation comprennent notamment les ordinateurs portables, les tablettes, les téléphones intelligents, les clés USB, les disques durs externes et les CD/DVD. Les données en transit sur Internet ou sur d'autres réseaux non protégés exigeant une protection peuvent comprendre les courriels, les pièces jointes des courriels, les données de sauvegarde pour le stockage hors site, les données provenant d'un site Web de l'organisation, et les données ou messages transmis à l'aide du protocole de transfert de fichiers (FTP) ou d'un programme de messagerie instantanée;

c) Les données sensibles doivent être protégées contre l'utilisation ou la divulgation non autorisées;

d) Les messages sensibles doivent être protégés contre la divulgation ou la mystification de l'expéditeur original (se faire passer pour lui).

2 OBJET

2.01 La présente directive a pour objet d'assurer la protection proactive des données sensibles afin de garantir :

- la confidentialité – protéger les données de l'accès et de la divulgation non autorisées;
- l'intégrité – s'assurer que les données ne sont pas modifiées en transit;
- la responsabilité – authentifier l'origine des données afin que l'expéditeur ne puisse nier qu'il les a envoyées.

3 PORTÉE

3.01 La présente directive s'applique :

a) au personnel de soutien technique de la TI qui examine les logiciels à mettre en œuvre;

b) au personnel des Opérations de la TI qui prépare les scripts pour une sauvegarde de système, que ce soit sur un support amovible ou pour le transfert par un réseau hostile;

c) aux utilisateurs finaux des systèmes de la TI qui transportent des données sensibles hors site sur un support amovible ou qui transfèrent des données sensibles en passant par un réseau hostile.

4 RESPONSABILITÉ

4.01 L'équipe de soutien technique de la TI doit :

a) évaluer périodiquement les exigences de chiffrement des données sensibles;

b) fournir des outils et des processus logiciels et matériels (p. ex. processus clés de génération et de gestion) pour faciliter le chiffrement;

c) fournir de la formation au personnel des Opérations de la TI et aux utilisateurs finaux pour leur permettre d'évaluer les données qui doivent être chiffrées et d'utiliser les outils fournis par l'organisation pour chiffrer leurs données efficacement.

4.02 Les employés des Opérations de la TI doivent :

a) cerner les données sensibles qu'ils stockent ou préparent à la transmission par un milieu hostile;

b) mettre en œuvre les outils fournis pour protéger les données en transit;

c) gérer les clés de chiffrement permettant le décodage de toutes les données chiffrées sous leur responsabilité.

4.03 Les utilisateurs finaux des systèmes de la TI doivent :

a) cerner les données sensibles qu'ils gèrent sur des ordinateurs partagés ou dans un milieu non sécurisé;

b) cerner les données sensibles qu'ils téléchargent sur un support amovible pour le transport ou le traitement hors site;

c) cerner les données sensibles qu'ils transmettent sur des réseaux non sécurisés (p. ex. courriels et pièces jointes des courriels);

d) chiffrer toutes les données sensibles pour chacun des cas susmentionnés, à l'aide des outils fournis par l'organisation;

e) gérer les clés de chiffrement conformément aux protocoles de l'organisation;

f) communiquer de façon sécurisée les clés de décodage aux destinataires approuvés des données chiffrées;

g) signaler les problèmes ou les défis concernant la mise en œuvre ou l'application des outils de chiffrement au soutien technique de la TI afin que des mesures correctives soient adoptées;

h) respecter toutes les autres politiques et procédures mises en œuvre concernant les pratiques de chiffrement.

5 DÉFINITIONS

5.01 Le **décodage des données** désigne le processus d'annulation de la transformation des données chiffrées pour pouvoir les lire normalement. (Voir **chiffrement des données** ci-dessous.)

5.02 Le **chiffrement des données** consiste à transformer les données en appliquant une formule ou un algorithme et à les stocker ou les transmettre dans l'état transformé afin que le matériel ne soit pas lisible, à moins que le lecteur sache comment renverser la transformation (c.-à-d. par le décodage des données).

5.03 Le **propriétaire des données** s'entend d'un cadre supérieur de l'organisation qui est responsable de la gestion générale d'un ensemble défini de données pour un secteur d'activités. Il a le pouvoir décisionnel quant aux personnes pouvant accéder aux données et les utiliser, et reçoit habituellement l'aide des gestionnaires de données. Le propriétaire des données approuve les processus et les politiques visant à maintenir la qualité des données et à normaliser les processus de gestion des données.

5.04 Un **milieu hostile** désigne un milieu pouvant compromettre la sécurité ou l'intégrité des données (les risques comprennent le vol et l'accès ou la modification non autorisé).

5.05 Une **clé** désigne un élément quelconque utilisé avec l'algorithme de chiffrement afin de chiffrer et de décoder de l'information. Il peut s'agir d'un mot de passe ou d'une phrase passe, ou d'un dispositif matériel ou d'un logiciel connu sous le nom de « jeton ». Pour un chiffrement plus sécuritaire, on peut appliquer plusieurs clés, comme un mot de passe et un jeton.

5.06 **Jeton**, voir **clé** ci-dessus.

5.07 Les **données sensibles** sont des données exigeant un haut niveau de confidentialité; elles sont « sensibles » à la divulgation non autorisée ou à la perte.

Le niveau désiré de confidentialité de ces données est la « sensibilité ». La sensibilité est fondée sur le calcul de l'atteinte à la réputation ou de la perte financière que la diffusion des données entraînerait.

6 DIRECTIVES CONNEXES

DCS TI 5.06 – Conservation des dossiers
DCS TI 9.03 – Contrôles de l'accès aux données
DCS TI 9.05 – Élimination des données
DCS TI 10.03 – Accès à distance
DCS TI 10.04 – Réseau sans fil
DCS TI 10.06 – Protocole de transfert de fichiers (FTP)
DCS TI 10.07 – Sécurité du courrier électronique
DCS TI 10.08 – Messagerie instantanée
DCS TI 10.09 – Commerce électronique
DCS TI 11.06 – Données de sauvegarde stockées hors site
DCS TI 13.07 – Supports amovibles
DCS TI 13.08 – Ordinateurs portables