OBJET

L'objet du présent document est de décrire les procédures et les lignes directrices à utiliser pour les employées et employés des conseils scolaires qui conservent ou transfèrent des informations personnelles et confidentielles à l'aide de moyens électroniques. Les présentes lignes directrices visent à assurer la confidentialité et l'intégrité des informations personnelles dans le cas où le cryptage des données serait utilisé comme mesure de protection. Elles visent également à donner des précisions qui favoriseront la compréhension des technologies de cryptage. Elles s'appliquent à tous les dispositifs, physiques ou virtuels, où l'on stocke des données des conseils scolaires. Les conseils scolaires peuvent utiliser ces lignes directrices pour élaborer des politiques ou des procédures relatives à l'utilisation du cryptage des données au sein de leur Conseil scolaire.

Définition

Le cryptage est un processus qui permet d'assurer la sécurité des informations personnelles et confidentielles. Il s'agit d'un procédé par lequel des segments de données sont mélangés mathématiquement à l'aide d'un mot de passe. Le processus de cryptage rend les données illisibles, à moins qu'elles ne soient décryptées ou jusqu'à ce qu'elles le soient.

Contexte

Le cryptage des données peut constituer une mesure efficace de protection pour la gestion des informations personnelles du personnel ou des élèves. Les employées et employés des conseils scolaires devraient comprendre que le cryptage des données ne remplace pas d'autres mesures de protection des informations telles que le contrôle de l'accès, l'authentification ou l'autorisation; que le cryptage des données devrait être utilisé conjointement avec ces autres contrôles; et que la mise en œuvre du cryptage des données devrait être proportionnelle aux besoins en matière de protection des données.

Applicabilité du cryptage

Transmission : Toute donnée classifiée comme étant personnelle et privée et pour laquelle il est nécessaire d'assurer la confidentialité et/ou l'intégrité devrait être transmise cryptée pour veiller à ce qu'elle ne traverse pas le réseau ou le Web en texte clair.

Les applications de cryptage pour la transmission des données comprennent, entre autres, les suivantes :

- **Transfert de fichier** – Le transfert crypté de fichier peut être effectué à l'aide d'un protocole de transmission ou service réseau crypté (p. ex. WinSCP, SFTP, etc.) ou en transférant un fichier qui a été crypté avant la transmission.

Dans le but d'alléger ce texte, le «Conseil scolaire» comprend aussi les administrations scolaires.

- **Courriel** – Le contenu confidentiel transmis dans les messages de courriel devrait être crypté avant la transmission, présenté par une application Web sécurisée ou cryptée dans un format de message sécurisé, compte tenu du fait que le courriel est exposé à la possibilité d'un accès non autorisé à un certain nombre de points tout au long du processus de livraison.
- **Sessions interactives** – Le cryptage de données privées, y compris les mots de passe d'ouverture de session, transmises durant les ouvertures de session à distance (p. ex. Telnet et les logiciels de télécommande d'ordinateurs personnels) devrait être assuré par l'utilisation d'applications ou de protocoles sécurisés.
- **Applications Web** – Le cryptage de données privées communiquées entre le navigateur d'un utilisateur et une application Web devrait être assuré par l'utilisation de protocoles sécurisés (p. ex. HTTPS, TLS/SSL, etc.). L'affichage des données devrait se limiter à ce qui est autorisé par l'utilisateur.
- **Communications à une imprimante de réseau** – Le cryptage des données privées transmises à une imprimante reliée à un réseau peut être assuré par l'utilisation d'applications d'impression (p. ex. JetDirect) ou de protocoles (p. ex. IPP) sécurisés pour empêcher l'interception non autorisée.
- **Services de fichiers distants** – Le cryptage des données privées transmises par les services de fichiers distants devrait être assuré par l'utilisation de protocoles de transmission cryptés (p. ex. IPSec, ISAKMP/IKE, SSL/TLS) pour empêcher l'interception non autorisée.
- **Accès à des bases de données** – Le cryptage des données privées transmises entre un serveur d'application et une base de données peut être mis en œuvre pour empêcher l'interception non autorisée. De telles capacités de cryptage font généralement partie intégrante du logiciel serveur de base de données ou sont offertes en option.
- **Communications application à application** – Le cryptage des données privées transmises entre des applications coopérantes devrait être assuré par l'utilisation de protocoles cryptés couramment accessibles (p. ex. SOAP avec HTTPS) pour empêcher l'interception non autorisée.
- **Réseau privé virtuel (RPV)** – Une connexion RPV offre une option supplémentaire pour protéger les données privées transmises par le réseau lorsque les autres solutions de rechange ne sont pas réalisables L'utilisation de RPV doit être étudiée attentivement de sorte que toutes les questions de sécurité et de réseautage soient comprises.

Stockage : Toute donnée classifiée comme étant personnelle et privée et pour laquelle il est nécessaire d'assurer la confidentialité et/ou l'intégrité devrait être transmise cryptée dans des systèmes et/ou des bases de données ou des appareils médias portatifs.

Les applications de cryptage aux fins de stockage des données comprennent, entre autres, les suivantes :

- **Cryptage de disque complet** – Le cryptage des données privées stockées sur des ordinateurs portatifs (p. ex. PDA, ordinateurs tablettes, ordinateurs bloc-notes et téléphones intelligents), ainsi que sur des supports de stockage (p. ex. lecteurs CD, DVD et USB) devrait être assuré par l'utilisation d'un outil de cryptage de disque complet ou d'un outil qui peut à tout le moins être configuré pour crypter toutes les données personnelles.
- **Cryptage de fichier** – Le cryptage de données privées devrait être effectué pour faciliter le transport sécuritaire des fichiers individuels sur un réseau sans cryptage des données transmises ou vers des dispositifs de stockage hors-ligne (p. ex. lecteurs CD, DVD ou USB.)

- **Stockage dans des bases de données** – Le cryptage des données privées contenues dans un serveur de base de données devrait être assuré par le cryptage de disque complet ou par l'utilisation des caractéristiques qui résident dans le logiciel du serveur de base de données. Les capacités de cryptage qui résident dans le logiciel du serveur de base de données peuvent permettre le cryptage de colonnes ou de tableaux particuliers d'une base de données et peuvent également être requises pour séparer les droits d'accès parmi plusieurs applications qui utilisent un seul serveur de base de données.
  - Le personnel qui conserve les données devrait comprendre que le cryptage du serveur de base de données ne veut pas dire que les données dans le serveur de base de données sont cryptées lorsqu'elles sont transmises sur un réseau. En général, le serveur de base de données décrypte les données avant leur transmission; par conséquent, le cryptage pour la transmission des données devrait également être mis en œuvre pour les serveurs de base de données qui traitent des données privées.
  - Le personnel qui conserve les données devrait tenir compte d'un certain nombre de facteurs lorsqu'il prend des décisions relativement au cryptage du serveur de base de données (p. ex. classification des données, besoin de confidentialité, nombre d'applications connexes, administration du système, performance, coût et exigences en matière de sauvegarde).
- **Sauvegarde et archivage** – Le cryptage des données privées contenues dans les copies de sauvegarde et/ou les fichiers d'archives devrait être assuré pour empêcher l'accès non autorisé.

Facteurs atténuants supplémentaires : Une combinaison de pratiques commerciales et de technologie peut réduire le risque d'exposition non autorisée des données et, de ce fait, réduire le besoin particulier de mettre en œuvre le cryptage des données.

Voici quelques exemples de facteurs atténuants :

- Capacités de restriction d'un pare-feu
- Journalisation détaillée des vérifications
- Journalisation détaillée des processus
- Capacités de détection d'intrusion
- Capacités de prévention d'intrusion
- Capacités de vérification de l'intégrité
- Séparation des tâches personnelles et confidentielles
- Capacités de sécurité physique

Services de cryptage

Les algorithmes symétriques devraient être utilisés pour crypter les informations privées. Le cryptage symétrique consiste à utiliser une seule et même clé pour le cryptage et le décryptage des données. Un canal sécurisé distinct est requis pour l'échange des clés. Voici des exemples d'algorithmes symétriques :

- AES (128, 192 ou 256 bits)
- RC6 (256 bits)
- Blowfish (128 ou 448 bits)

- Triple DES (112 ou 168 bits)
- RC4-128
- IDEA-128
- CAST-128
- RC5 (128 bits seulement)
- SAFER (128 bits)

Les algorithmes asymétriques devraient être utilisés pour le cryptage à clé publique de données privées. Le cryptage asymétrique consiste à utiliser une paire de clés pour le cryptage et le décryptage des données. L'expéditeur du message crypte le message à l'aide de la clé publique du destinataire. Le destinataire décrypte ensuite le message à l'aide de sa clé privée. Voici des exemples d'algorithmes asymétriques à clé publique :

- RSA (minimum de 1 024 bits)
- ECC (minimum de 384 bits)

Les signatures numériques devraient être utilisées pour associer un utilisateur ou une entité avec une clé publique respective. Une clé publique est la clé publiquement accessible d'une paire de clés de signature qui est utilisée pour valider une signature numérique et/ou pour crypter des informations confidentielles. Les services de cryptage suivants devraient être utilisés aux fins de signature numérique lorsque des informations privées sont en cause :

- RSA (minimum de 1 024 -bits) avec SHA-1
- DSA (minimum de 1 024 bits) avec SHA-1
- ECDSA (minimum de 384 bits) avec SHA-1

Les certificats numériques devraient appliquer les normes reconnues (p. ex. X.509v3) et devraient à tout le moins :

- Identifier l'autorité de certification émettrice – l'autorité de certification devrait être un organisme autorisé par la politique de gestion des documents ou strictement désigné pour l'usage interne du Conseil scolaire;
- identifier la personne (l'abonné) qui est l'entité ou le sujet désigné nommé ou identifié dans un certificat délivré à cette personne et qui possède une clé privée, laquelle correspond à la clé publique indiquée dans le certificat;
- fournir la clé publique de l'abonné;
- identifier sa période opérationnelle;
- être signés numériquement par l'autorité de certification émettrice.

Gestion des clés de cryptage

1. Les clés de cryptage utilisées pour protéger des données personnelles devraient également être considérées comme des données personnelles.
2. La gestion professionnelle des clés est essentielle pour empêcher la divulgation non autorisée de données personnelles ou la perte irréparable de données importantes. On devrait mettre à la disposition de tout le personnel des conseils scolaires une infrastructure centralisée de gestion de clés des conseils scolaires pour s'assurer que les contrôles appropriés sont appliqués. Les données des conseils scolaires gérées par toutes les infrastructures de gestion de clés devraient être considérées comme étant à la fois personnelles et cruciales à la mission.

3. Toutes les infrastructures de gestion de clés des conseils scolaires devraient créer et mettre en œuvre un plan de gestion des clés de cryptage pour répondre aux exigences des présentes lignes directrices sur le cryptage, d'autres politiques des conseils scolaires et des lois sur l'éducation ou la protection des informations personnelles applicables.

- Le plan de gestion des clés de cryptage devrait garantir la possibilité de décrypter les données lorsque l'accès à celles-ci est nécessaire. Un plan de secours ou d'autres stratégies (p. ex. agents de récupération, etc.) devraient être mises en œuvre pour permettre le décryptage et ainsi s'assurer de pouvoir récupérer les données en cas de perte ou de non disponibilité des clés de cryptage.
- Le plan de gestion des clés de cryptage devrait aborder la compromission ou la compromission soupçonnée des clés de cryptage. Le plan devrait indiquer les mesures à prendre en cas de compromission (p. ex. avec les logiciels et le matériel du système, les clés privées ou les données cryptées).
- Le plan de gestion des clés de cryptage devrait également aborder la destruction ou la révocation des clés de cryptage qui ne sont plus utilisées (p. ex. l'utilisateur a quitté le Conseil scolaire) ou qui ne sont pas associées à un programme de gestion des clés.

4. Toutes les clés de cryptage symétrique utilisées sur des systèmes associés à des données personnelles devraient être générées au hasard conformément aux normes de l'industrie. Les normes acceptables comprennent, entre autres, les suivantes :

- FIPS 186-2
- ANSI X9.31
- ANSI X9.62
- ANSI X9.82

5. Dans les cas où le cryptage symétrique est utilisé pour protéger des données personnelles :

- Les clés maîtresses (clés utilisées pour dériver d'autres clés symétriques) devraient être remplacées au moins une fois par année.
- Les clés de cryptage de clés (clés utilisées pour crypter d'autres clés à l'aide d'algorithmes à clés symétriques) devraient être remplacées au moins deux fois par année.
- Les clés de cryptage de données (clés utilisées avec des algorithmes à clés symétriques pour appliquer la protection de la confidentialité des informations) devraient être remplacées une fois par session ou toutes les 24 heures.

6. Lorsque le cryptage asymétrique est utilisé, la période opérationnelle des clés asymétriques associées à un certificat de clé publique est définie par le plan de gestion des clés de cryptage de l'autorité de certification émettrice.

7. Les clés de cryptage devraient être stockées dans un dépôt de clés cryptées ou sous forme autrement cryptée à l'aide d'algorithmes approuvés, ou bien elles peuvent être stockées sur un jeton de sécurité (p. ex. une carte intelligente). Les clés de cryptage ne devraient jamais quitter le dispositif si elles sont stockées sur un jeton de sécurité.
   - Cette exigence ne s'applique pas aux clés (p. ex. clés d'hôtes SSH) ni aux protocoles (p. ex. cryptage utilisé par les technologies de sauvegarde) qui fournissent des couches de transport de cryptage en plus du cryptage fort qui a déjà été appliqué aux données personnelles.
8. Les clés de cryptage sont des informations confidentielles, et l'accès à celles-ci devrait être strictement réservé aux personnes qui ont besoin de savoir. Le ou les propriétaires des données protégées par des services de cryptage devraient clairement assigner la responsabilité de la gestion des clés de cryptage devant être utilisées pour protéger ces données. Les clés transmises sur des lignes de transmission devraient être sous forme cryptée. L'échange des clés devrait utiliser un algorithme de cryptage plus fort que celui utilisé pour crypter les données protégées par les clés.
9. Les clés de cryptage qui sont compromises (p. ex. perdues ou volées) devraient être signalées immédiatement au bureau du Conseil scolaire, au gestionnaire des clés et au propriétaire des données en question. On devrait révoquer ou détruire la clé et en produire une nouvelle. Les réaffectations de clés devraient nécessiter le recryptage des données.

Autorités de certification

1. Les clés de cryptage produites par une autorité de certification (AC) et utilisées pour contrôler l'accès au serveur de l'AC ou utilisées par l'AC pour exécuter des fonctions devraient être stockées sur des modules de sécurité matérielle (HSM).
2. Tous les HSM utilisés au sein du Conseil scolaire devraient adhérer à des normes reconnues (p. ex. FIPS 140-3).
3. Les AC des conseils scolaires doivent être conçues de sorte que toutes les fonctions des administrateurs de l'AC soient justifiées en détail. Idéalement, aucun administrateur ne devrait obtenir, à lui seul, l'accès complet aux clés de cryptage des AC (p. ex. les mesures d'accès devraient comprendre la séparation des tâches, le double contrôle, etc.).
4. Les AC des conseils scolaires au sein du Conseil devraient adhérer à un plan de gestion des clés de cryptage.

Références

Université du Texas – *UT Austin Data Encryption Guidelines*
http://www.utexas.edu/its/policies/opsmanual/encrypt-guide.php

UT-Austin: IT Security Operations Manual

UT-Austin: Data Classification Standard

UT-Austin: Minimum Security Standards for Systems

UT-Austin: Minimum Security Standards for Data Stewardship

NIST Special Publication 800-57:

Recommendation for Key Management, Part 1 et Recommendation for Key Management, Part 2

Parties adaptées de *University of Pittsburgh: Security Guidelines for Encryption*

(http://technology.pitt.edu/documentation/Security_Guidelines/Encryption_Guideline-vs-2.0.pdf), avec la permission de l'Université de Pittsburgh, Pittsburgh, Pennsylvanie 15260-3332

Parties adaptées de *Encryption at the University of California: Overview and Recommendations* (http://www.ucop.edu/irc/itsec/uc/EncryptionGuidelinesFinal.html), avec la permission du bureau du président de l'Université de Californie, Oakland, Californie 94607-5200.

Université McMaster – glossaire de Campus Technology Liaison : www.mcmaster.ca/ctl/glossary.htm