Cree School Board
ᐃᔨᔫ ᒋᔅᑯᑎᒫᑳᐅᓐ
Commission Scolaire Crie

Politique relative à l'intervention de la Commission scolaire crie en cas d'atteinte à la sécurité des systèmes d'information

Service responsable : Technologies de l'information
Date en vigueur : 1 juillet 2012
Amendée le : 1er décembre 2013 et le 4e février 2016
Approuvées par : Résolution #EC 2016-037

Références :	Council Policy Manual: ▪ *EL - General Executive Constraints* ▪ *EL 1 - Treatment of Students and Parents* ▪ *EL 2 - Treatment of Employees* ▪ *EL 5 - Asset Protection*

1) BUT ET PORTÉE

But

1.1. La présente politique décrit le protocole à suivre à l'égard d'une atteinte à la sécurité où il est raisonnable de croire qu'une personne non autorisée a obtenu ou a eu accès à de l'information organisationnelle ou personnelle traitée et gérée par la Commission scolaire crie.

Portée

1.2. Il sera raisonnable de croire qu'une personne non autorisée a obtenu ou a eu accès à de l'information organisationnelle ou personnelle dans les cas qui suivent :

a) perte ou vol de documents imprimés;

b) perte ou vol de tout système ou appareil informatique (serveur, ordinateur portable ou de bureau, assistant numérique personnel (PDA), ou téléphone cellulaire contenant de l'information organisationnelle ou personnelle non cryptée);

c) perte ou vol de médias numériques (*thumb drives*, clés USB, cartes mémoire, supports optiques tels que CD ou DVD), ou de cartes SD contenant de l'information organisationnelle ou personnelle non cryptée;

d) tentative réussie de piratage ou d'intrusion illégale par le biais du réseau de systèmes informatiques;

e) accès non autorisé à des données par tout autre moyen – accès, visualisation, téléchargement ou obtention d'information organisationnelle ou personnelle non cryptée gérée par la CSC par une personne qui n'est pas autorisée à accéder à ces données. Ceci couvre aussi les situations où une personne a reçu des données qu'elle n'est

pas autorisée à accéder ou à voir, tels courriels ou documents sur papier transmis au mauvais destinataire, mauvaise configuration des paramètres d'accès et, enfin, obtention illégale de codes d'accès et de mots de passe de courriels d'employés et/ou de comptes d'utilisateurs dans le réseau.

Objectifs

1.3. La présente politique vise à s'assurer que :

- les événements et les incidents sont systématiquement classés, mis en corrélation, priorisés, assignés et analysés
- les interventions en cas d'incident compromettant la sécurité sont coordonnées et traitées de manière cohérente
- les personnes ou les services dont l'information est obtenue sont avisés en temps opportun
- les stratégies d'atténuation et les améliorations à la sécurité de l'organisation sont constamment examinées et mises en œuvre pour éviter de futurs incidents similaires.

Coordination

1.4. Le Service des technologies de l'information de la CSC (STI) coordonnera l'examen de toute atteinte à la sécurité pouvant avoir donné un accès non autorisé à de l'information électronique organisationnelle ou personnelle.

2) Définitions

Définitions

2.1. Dans la présente politique, on entend par :

a) **Atteinte à la sécurité :** acquisition non autorisée de données électroniques ou sur papier qui compromet la sécurité, la confidentialité ou l'intégrité de l'information organisationnelle ou personnelle conservée par la CSC. Cela ne comprend pas l'acquisition de bonne foi d'information personnelle par un employé ou un mandataire de la CSC, en autant que l'information personnelle n'est pas soumise à une utilisation ou divulgation non autorisée;

b) **Donnée organisationnelle :** tout élément de donnée de nature privée, vitale, et permanente qui appartient exclusivement à la CSC, qui s'inscrit dans son mandat et qui est limité à un usage interne;

c) **Donnée cryptée :** donnée qui a été suffisamment modifiée de manière à la rendre inintelligible pour toute personne non autorisée;

d) **Information personnelle :** prénom ou initiale et nom d'une personne, combinés avec un ou plusieurs des éléments de données qui suivent, lorsque le nom et/ou les éléments de données ne sont pas cryptés :

- numéro d'assurance-sociale (NAS), ou numéro d'employé
- numéro de permis de conduire ou autre carte d'identification personnelle
- numéro de compte (qui pourrait inclure un numéro d'identification de l'élève), numéro de carte de crédit ou de débit, combiné avec le code de sécurité, le code d'accès, ou le mot de passe qui permettrait l'accès au compte d'une personne

e) **Unité administrative :** chacun des services au sein de la CSC;

f) **Utilisateurs de données :** employés, élèves, conseillers et autres personnes qui gèrent fréquemment ou rarement, dans le cadre de leurs fonctions régulières, de l'information organisationnelle électronique qui appartient à la CSC;

g) **Équipe d'intervention en cas d'incident :** groupe composé de membres de l'équipe des technologies de l'information dont le mandat est de répondre à toute atteinte à la sécurité;

h) **Donnée non cryptée :** donnée en texte brut ou clair et intelligible par toute partie sans devoir la déchiffrer (par exemple : courriels).

3) RESPONSABILITÉS

Les personnes et les unités administratives qui suivent ont les obligations de rendre compte et les responsabilités décrites ci-après :

Services

3.1. Chaque unité administrative doit :

a) informer les utilisateurs autorisés à accéder à l'information organisationnelle ou personnelle de leurs responsabilités de protéger ces données contre une divulgation non autorisée;

b) établir des procédures de surveillance pour bien identifier et intercepter les accès non autorisés ou les activités anormales conformément aux lignes directrices du STI;

c) signaler tout soupçon d'une acquisition ou d'un accès non autorisé à de l'information organisationnelle ou personnelle au directeur du STI, au directeur des ressources humaines et au directeur général.

Utilisateurs

3.2. Tout utilisateur doit :

a) se conformer aux procédures et politiques sur l'accès et l'utilisation de l'information organisationnelle ou personnelle;

b) protéger les ressources sous sa responsabilité, telles que mots de passe, ordinateurs et données qu'il a téléchargées et stockées;

c) signaler à son superviseur, ainsi qu'au STI, toute acquisition non autorisée ou activité irrégulière qui peut avoir entraîné ou rendu possible la divulgation d'information organisationnelle ou personnelle à des personnes non autorisées.

Reddition de compte

3.3. Le directeur du STI gère toute atteinte à la sécurité de l'information organisationnelle ou personnelle. Ses responsabilités comprennent, sans s'y limiter :

a) décider de la nécessité d'une équipe d'intervention en cas d'incident composée de membres nommés (dont un coordonnateur et d'autres membres de l'équipe des TI);

b) voir à ce que d'autres ressources adéquates et appropriées soient affectées en vue de répondre et de résoudre l'incident (temps, tierces parties si nécessaires, etc.);

c) communiquer efficacement avec les utilisateurs et les unités administratives touchés;

d) tenir l'équipe d'intervention en cas d'incident qui a été assignée informée de l'état courant de l'incident;

e) encadrer et aider l'équipe d'intervention en cas d'incident dans ses efforts visant à identifier l'atteinte à la sécurité et à y remédier;

f) veiller à ce que la présente politique soit appliquée, y compris formuler des recommandations à l'égard d'évaluation spécifique, d'enquête, de mesures d'atténuation, de procédures de signification d'avis, et de communications au Comité de gestion;

g) sur demande, présenter les résultats en cours dans le ou les rapports écrits au directeur général;

h) déposer un rapport de clôture au directeur général une fois l'incident géré, confiné et résolu.

4) Procédure d'intervention en cas d'incident

Atteinte présumée	Intervention en cas d'incident	Examen de l'incident	Signification d'avis	Production de rapport

Atteinte présumée

4.1. Toute atteinte présumée à un système contenant de l'information organisationnelle ou personnelle doit être signalée au STI par toutes les parties qui en ont connaissance. Le directeur du STI, en partenariat avec l'équipe d'intervention en cas d'incident et, peut-être, avec l'unité administrative qui gère ou utilise des fonctionnalités de tout système d'information ou support touché, confirme l'atteinte à la sécurité.

4.2 Le directeur général (soit le directeur général ou une personne de son bureau qu'il nomme pour cette tâche) tiendra compte des constatations et des faits que lui présentent le directeur du STI et l'équipe d'intervention en cas d'incident pour décider des modalités de notification de l'avis (p. ex. courriel, courrier postal ou avis sur site Web).

4.2.1 Si le directeur général détermine que la signification d'un avis est nécessaire, et l'autorise, l'unité administrative doit aviser sans délai toute personne touchée de la divulgation possible d'information.

4.2.2 Suite à un incident, la CSC peut s'attendre à plusieurs demandes de renseignements de la part d'utilisateurs avisés, ou de leurs parents, conjoints,

membres de la famille, ou amis, etc. Le directeur TI fournira des lignes directrices que la ou les personnes désignées du service concerné doivent suivre quand elles répondent à des appels téléphoniques, courriels, lettres, ou visites spontanées portant sur l'incident. En général, les lignes directrices sur les incidents demandent aux employés :

a) de ne pas offrir de l'information ou des commentaires non sollicités aux médias publics;

b) d'informer la personne qui fait la demande que l'incident est sous enquête (si c'est le cas);

c) d'orienter la personne qui fait la demande vers une section du site Web ou un employé pour obtenir de l'information sur l'incident;

d) d'orienter les personnes des forces de police qui font la demande directeur général;

e) d'orienter les personnes des médias qui font la demande au bureau du directeur général ou à un employé nommé par le DG en tant que directeur des relations publiques pour l'organisation.

5) Application de la présente politique

Dispositions antérieures

5.1. La présente politique remplace toute autre politique de la Commission relative à ce sujet, respectant toutefois, le cas échéant, les politiques/ends adoptées par le Conseil des commissaires.

Version officielle

5.2. La secrétaire générale de la Commission conserve la version officielle de la présente politique.

Responsabilité

5.3. Toute personne visée par la présente politique doit en respecter l'ensemble des dispositions. Tous les gestionnaires de la Commission scolaire sont responsables de l'application et du respect de l'ensemble des dispositions de la présente politique.

Le directeur du Service des technologies de l'information est la personne responsable de fournir un soutien à l'interprétation de la présente politique et de veiller à sa mise à jour, s'il y a lieu.