Cree School Board
Commission scolaire crie

Policy regarding the Cree School Board Information Systems Security Breach Response

Department responsible: Information and Technologies
Effective date: July 1, 2012
Amended on: December 1, 2013 and February 4, 2016
Approved by*:* Resolution # EC 2016-037

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

1) Purpose and Scope

Purpose

1.1. This Policy outlines the protocol for responding to a security breach in which it is reasonably believed that corporate or personal information processed and maintained by the Cree School Board has been acquired or accessed by an unauthorized party.

Scope

1.2. Corporate or personal information will be reasonably believed to have been acquired by an unauthorized party if any of the following situations occur:

a) Loss or theft of printed documents;
b) Loss or theft of any computing system or device (any server, desktop, laptop, personal digital assistant (PDA), or cell phone containing unencrypted corporate or personal information);
c) Loss or theft of digital media (thumb drives, memory sticks / cards, optical media such as CDs or DVDs), or SD cards containing unencrypted corporate or personal information;
d) A successful hacking incident or illegal intrusion via the network of computer systems;
e) Unauthorized data access through any other means - Accessing, viewing, downloading or otherwise obtaining unencrypted corporate or personal information maintained by the CSB by individuals who do not have the proper authorization to access that data. This includes situations where individuals have received data that they are not authorized to access or review, such as emails or paper documents sent to the wrong recipient, incorrect computer access settings, and

finally, illegal procurement of access codes and passwords of employee e-mail and/or network accounts.

Objectives

1.3. The objectives of this Policy are to ensure that:

- Events and incidents are systematically categorized, correlated, prioritized, assigned, and analyzed
- Responses to security events are coordinated and dealt with in a consistent fashion
- Individuals or departments whose information is acquired are notified in a timely manner
- Mitigation strategies and enhancements to the organization's security are constantly examined and implemented to avoid future similar security events.

Coordination

1.4. The CSB's Information & Technologies Services (ITS) will coordinate the review of any security breach that potentially involves unauthorized access to corporate or personal electronic information.

2) Definitions

Definitions

2.1. In this Policy, the following words or expressions mean:

a) **Breach of security**: a breach of security is the unauthorized acquisition of paper or computerized data compromising the security, confidentiality, or integrity of corporate or personal information maintained by the CSB. This does not include good faith acquisition of personal information by an employee or agent of the CSB, if the personal information is not used or subject to any subsequent unauthorized disclosure;

b) **Corporate data**: any data elements which are solely owned by the CSB which are private, vital, permanent and within the organization's mandate and which are limited to internal use;

c) **Encrypted data**: data that has been sufficiently altered so as to be unintelligible to any unauthorized parties;

d) **Personal information**: personal information means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name and/or the data elements are not encrypted:

- Social Insurance Number (SIN), or employee number
- Driver's license number or other personal identification card
- Account number (which could include a student identification number), credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's account

e) **Departmental units**: departments within the organization;

f) **Data users**: employees, students, consultants and others who handle either frequently or infrequently, as part of their regular duties, CSB-owned electronic corporate information;

g) **Incident response team**: a group composed of members of the Information & Technologies team whose mandate is to respond to any breach of security;

h) **Unencrypted data**: data that is in plain or clear text and understandable by any party without the need to decrypt (e.g: e-mail messages).

3) RESPONSIBILITIES

The following individuals and departmental units have the following accountabilities and responsibilities:

Departments

3.1. All departmental units must:

a) inform users that are granted access to corporate or personal information of their responsibilities to secure such data from unauthorized release;

b) establish monitoring procedures to correctly identify and intercept unauthorized access or anomalous activity according to ITS department defined global guidelines;

c) report any suspected unauthorized activity or potential acquisition of corporate or personal information to the Director of ITS, the Director of Human Resources and the Director General.

Data Users

3.2. All data users must:

a) abide by established procedures and policies pertaining to access to and usage of corporate or personal information;

b) protect resources under their control such as passwords, computers, and data they have downloaded and stored;

c) report to their respective supervisors as well as to ITS any unauthorized acquisition or irregular activities which may have resulted in, or created the potential to release corporate or personal information to unauthorized individuals.

Accountability

3.3. The officer in charge of handling a security breach involving corporate or personal information will be the Director of ITS. His responsibilities include but are not limited to:

a) invoking the need for an incident response team composed of appointed members (including a coordinator and other members of the ITS Team);

b) ensuring additional adequate and appropriate resources are assigned to respond and resolve the incident (time, third parties as necessary, etc.);

c) executing effective communication to affected users and departmental units;

d) keeping the assigned incident response team informed of incident status;

e) supervising and assisting the incident response team in its effort to identify and resolve the security breach;

f) ensuring that this policy and processes are followed, including recommending specific assessment, investigation, mitigation steps, notification procedures, and management group communication;

g) submitting ongoing findings in written report(s) to the Director General as required;

h) tabling a closure report to the Director General once the incident has been successfully managed, contained and resolved.

4) Security Incident Response Procedure

Suspect breach

4.1. Any suspected breach of a system containing corporate or personal information must be reported to the ITS by all parties who have any knowledge thereof. The Director of ITS, in partnership with the incident response team and possibly the departmental unit involved in managing or using the functionalities of any affected information systems or media, will confirm the security breach.

4.2 The Director General (either the Director General or a person within the DG's department assigned by the DG for this task) will consider, based on findings and facts provided by the Director of ITS and the incident response team, what means of notification (e.g. e-mail, postal mail or website notice) should be used.

4.2.1 If the Director General determines and authorizes that notification is required, the departmental unit must notify any affected individual(s) of the possible information release without unnecessary delay.

4.2.2 Subsequent to an incident, the CSB can expect several inquiries from notified users, or their parents / spouses / family members / friends, etc. The Director of ITS will provide guidelines to be used by the individual(s) designated in the affected department for their response to any phone calls / e-mails / letters / walk-in traffic involving inquiries regarding the incident. In general, the incident guidelines will direct employees:

a) Not to offer unsolicited information or comments to the public media;

b) To advise the inquirer that the incident is under investigation (if this is the case);

c) To direct the inquirer to a web site section or an employee for incident information;

d) To direct inquirers from law enforcement authorities to the Director General;

e) To direct inquirers from the media to the Director General or to an employee appointed by the DG as a Public Relation Officer for the organization.

5) Application of this Policy

Previous provisions

5.1. This Policy replaces all other policies of the Board pertaining to this subject while respecting the policies/Ends adopted by the Council of Commissioners where applicable.

Official version

5.2. The official version of this Policy is kept by the Secretary-General of the Board.

Responsibility

5.3. Any person referred to in this Policy must abide by all its provisions. All managers of the School Board are responsible to ensure that all of its provisions are applied and respected.

The Director of Information and Technologies is the person responsible for providing support in the interpretation of this Policy and to ensure its revision when necessary.