

Titre : POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

1. CONTEXTE

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, Loi 133) et de la Directive sur la sécurité de l'information gouvernementale crée des obligations aux commissions scolaires en leur qualité d'organismes publics.

Ainsi, la Directive sur la sécurité de l'information gouvernementale oblige la commission scolaire à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information en ayant recours, notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Cette politique permet à la Commission scolaire de la Rivière-du-Nord (CSRDN) d'accomplir ses missions, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue. Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, intégrité ou confidentialité peuvent avoir des conséquences liées à :

- La vie, la santé ou le bien-être des personnes;
- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- L'image de la commission scolaire et du gouvernement.

2. OBJECTIF DE LA POLITIQUE

La présente politique a pour objectif d'affirmer l'engagement de la commission scolaire de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou son moyen de communication. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

3. CADRE NORMATIF

La politique de sécurité s'inscrit principalement dans un contexte régi par :

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- La Loi sur l'instruction publique (LRQ, c. I-13.3);
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (LRQ, c. A-21.1, r.1);
- Le Code civil du Québec (LQ, 1991, chapitre 64);

- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, Loi 133);
- La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- Le Code criminel (LRC, 1985, chapitre C-46);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1. r.2);
- La Directive sur la sécurité de l'information gouvernementale;
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- La Politique 8208 relative à la collecte, la conservation et l'utilisation des renseignements nominatifs et à la protection des renseignements personnels;
- La Politique 7111 relative à la gestion du réseau informatique de la CSRDN;
- La Politique 7113 relative à l'utilisation des technologies de l'information;
- La Politique 7110 relative à l'utilisation des médias sociaux.

4. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs, c'est-à-dire à tout le personnel, peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de bénévole, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels de la commission scolaire ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que la commission scolaire détient dans l'exercice de ses fonctions, que sa conservation soit assurée par elle-même ou par un tiers.

5. DÉFINITIONS

Actif informationnel

Une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par la commission scolaire habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

Catégorisation

Le processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant son degré de sensibilité en termes de disponibilité, d'intégrité et de confidentialité et, par conséquent, le niveau adéquat de protection à lui accorder.

Confidentialité

Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information

L'ensemble des étapes que franchit l'information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation de la commission scolaire.

Détenteur de l'information

La direction d'un service ou d'un établissement qui a la garde d'actifs informationnels de la commission scolaire ou tout autre gestionnaire à qui cette responsabilité a été déléguée.

Disponibilité

La propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

Incident

Un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

Incident de sécurité de l'information à portée gouvernementale

La conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale dont les risques d'atteinte à sa disponibilité, à son intégrité ou à sa confidentialité peuvent avoir des conséquences liées à la vie et la santé ou le bien-être des personnes, à l'atteinte à la protection des renseignements personnels et à la vie privée, à la prestation de services à la population ou à l'image de la commission scolaire et du gouvernement et nécessitant une intervention concertée au plan gouvernemental.

Information

Un renseignement consignés sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Intégrité

Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Plan de continuité

L'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité de la Commission scolaire.

Plan de relève

Le plan de reprise hors site mis en œuvre lorsqu'il y a détérioration ou destruction d'actifs informationnels consécutive à un incident exigeant le transfert de l'exploitation dans un autre lieu.

Le plan de relève décrit les procédures visant à assurer, dans des conditions de continuité adaptées aux critères de survie de la Commission scolaire, la mise à la disposition rapide et ordonnée des moyens de secours ainsi que la reprise éventuelle de l'exploitation normale après réfection ou remplacement des actifs détruits ou endommagés.

Risque de sécurité de l'information

Le degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de réduction de la qualité des services ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ou sur l'image de la Commission scolaire.

Risque de sécurité de l'information à portée gouvernementale

Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

Sécurité de l'information

La protection de l'information et des systèmes d'information contre les risques et les incidents.

6. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions de la commission scolaire en matière de sécurité de l'information sont les suivants :

- a) S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité.
- b) Reconnaître l'importance de la politique de sécurité de l'information.
- c) Reconnaître que l'environnement technologique des actifs de l'information numérique et non numérique est en changement constant et interconnecté avec le monde.
- d) Protéger l'information tout au long de son cycle de vie.
- e) S'assurer que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales.
- f) Sensibiliser et former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

7. GESTION DES RISQUES

Une catégorisation à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

La gestion des risques liés à la sécurité de l'information numérique et non numérique s'inscrit dans le processus global de gestion des risques de la commission scolaire. Les risques à portée gouvernementale sont déclarés conformément à la Directive sur la sécurité de l'information

gouvernementale. L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de la commission scolaire.

Le niveau de protection de l'information est établi en fonction :

- De la nature de l'information et de son importance.
- Des probabilités d'accident, d'erreur ou de malveillance auxquelles elles sont exposées.
- Des conséquences de la matérialisation de ces risques.
- Du niveau de risque acceptable par la commission scolaire.

8. GESTION DES INCIDENTS

La commission scolaire déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, elle met en place les mesures nécessaires à l'obtention des buts suivants :

- Limiter l'occurrence des incidents en matière de sécurité de l'information.
- Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés au ministère de l'Éducation et de l'Enseignement supérieur (MEEES) conformément à la Directive sur la sécurité de l'information gouvernementale.

9. CULTURE DE SÉCURITÉ ET CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

L'atteinte des objectifs de sécurité de l'information requiert l'octroi de responsabilités à tous les niveaux de l'organisation et la mise en place d'un processus de gestion permettant une organisation fonctionnelle de la sécurité de l'information par tous les acteurs visés par cette politique et par les comités chargés de la sécurité de l'information, de la gestion des incidents et de la continuité des services. Dans cette dernière perspective, la CSRDN établit un cadre de gestion de la sécurité de l'information.

10. PLAN DE RELÈVE ET PLAN DE CONTINUITÉ

Dans le but d'assurer la disponibilité des services critiques, la CSRDN doit s'assurer de maintenir et d'actualiser périodiquement un plan de relève ainsi qu'un plan de continuité afin de minimiser les impacts d'une crise ou d'une catastrophe naturelle, sociale ou technologique. Ces plans couvrent différents scénarios permettant notamment de se préparer à la non-disponibilité des actifs informationnels ou du personnel.

11. DROIT DE REGARD ET D'INTERVENTION

Pour garantir la sécurité de ses actifs informationnels, la CSRDN se réserve un droit de regard et d'intervention sur toute activité susceptible d'affecter ces derniers. Les accès aux actifs informationnels, réussis ou refusés, sont surveillés et journalisés afin de permettre de futures vérifications.

Des enquêtes sur les actions d'un utilisateur peuvent être enclenchées si une demande est justifiée et approuvée par un gestionnaire supérieur.

Ce droit de regard est exercé conformément au cadre légal et normatif applicable et au respect de la vie privée.

12. ÉCRITS DE GESTION

La CSRDN devra maintenir et actualiser périodiquement des écrits de gestion posant des balises, des attentes ou procédures notamment relativement à la gestion des accès, à la gestion des vulnérabilités, à la gestion des copies de sauvegarde, à la protection du périmètre réseau, aux mandats ou aux contrats avec les fournisseurs.

13. SANCTIONS

Tout utilisateur qui contrevient à la présente politique s'expose à des interventions et/ou des mesures disciplinaires, administratives ou légales.

14. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le conseil des commissaires et remplace la politique 7112 *Politique relative à la sécurité des actifs informationnels*.