Commission scolaire
de la Rivière-du-Nord

POLITIQUE

No **7112**

Titre : POLITIQUE RELATIVE À LA SÉCURITÉ DES ACTIFS INFORMATIONNELS

1. INTRODUCTION

1.1 Objectifs

La politique de sécurité des actifs informationnels exprime la prise de position de la Commission scolaire de la Rivière-du-Nord concernant les mesures de sécurité considérées comme essentielles à la protection de ses actifs informationnels. Elle regroupe les énoncés de principes généraux et les rôles et responsabilités des intervenants ainsi que les orientations de la Commission touchant les règles d'accès aux actifs informationnels, la gestion de l'information et les mesures de sécurité et d'urgence.

1.2 Champs d'application

1.2.1 Actifs visés : Cette politique s'applique aux quatre catégories d'actifs informationnels suivants :

- ceux appartenant à la Commission et exploités par cette dernière;
- ceux appartenant à la Commission et exploités ou détenus par un fournisseur de services ou un tiers;
- ceux appartenant à un fournisseur des services ou un tiers et exploités par lui au profit de la Commission;
- ceux n'appartenant pas à la Commission et exploités ou détenus par la Commission.

1.2.2 Personnes visées : Cette politique s'adresse à tout le personnel de la Commission de quelque statut qu'il soit, ainsi qu'à toute personne dûment autorisée qui a recours à l'actif informationnel de la Commission dans l'exercice de ses fonctions. Les consultants, partenaires, bénévoles et fournisseurs utilisant et ayant accès aux biens de la Commission ou ayant des biens de la Commission sous leur garde, ont les mêmes obligations que le personnel de la Commission.

1.2.3 Activités visées : Toutes les activités impliquant la manipulation ou l'utilisation sous toutes ses formes des actifs informationnels de la Commission sont visées par la présente politique, que celles-ci soient conduites dans ses locaux, dans un autre lieu ou à distance.

1.3 Définitions

1.3.1 Actif informationnel : Une information numérique, une banque d'information numérique, un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par une organisation.

1.3.2 **Commission** : Commission scolaire de la Rivière-du-Nord

1.3.3 **Confidentialité** : Propriété d'une information de n'être accessible qu'aux personnes autorisées.

1.3.4 **Continuité** : Propriété qu'ont les ressources informationnelles d'être accessibles de la manière requise (sans interruption, délai ou dégradation) et utilisables au moment voulu.

1.3.5 **Courriel** : Service de correspondance sous forme d'échange de messages électroniques à travers un réseau de télécommunications.

1.3.6 **Cycle de vie de l'information numérique** : Période de temps couvrant toutes les étapes d'existence de l'information numérique dont celles de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information.

1.3.7 **Détenteur** : Gestionnaire ou autre membre du personnel de la Commission à qui est assignée la responsabilité de la sécurité d'un actif informationnel et/ou d'un processus d'affaires.

1.3.8 **Disponibilité** : Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

1.3.9 **Document technologique** : Information délimitée et structurée de façon logique sur un support faisant appel aux technologies de l'information, intelligible sous forme de mots, de sons ou d'images. Est assimilée au document technologique toute banque de données dont les éléments structurants permettent la création de documents par la délimitation ou la structuration de l'information qui est inscrite[1].

1.3.10 **Équipement informatique** : Tout équipement de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information et tout équipement de télécommunication.

1.3.11 **Fichier** : Collection d'information consignée et stockée comme une entité unique et spécifique sur un support de stockage.

1.3.12 **Habilitation** : Fonction permettant d'attribuer à un utilisateur l'autorisation de porter des actions sur les ressources.

1.3.13 **Information numérique** : Information dont l'usage n'est possible qu'au moyen de technologies de l'information.

1.3.14 **Inforoute** : Réseau étendu d'information à haut débit et à grande vitesse, capable de transmettre des données de toutes sortes, notamment des données multimédias, et destiné à jouer le rôle d'infrastructure globale de communication au service de l'ensemble des populations, sur les plans national et international.

1.3.15 **Intégrité** : Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation. L'intégrité fait référence à l'exactitude ou à l'état complet de l'information.

[1] Articles 1 (2°) et 3 de la Loi concernant le cadre juridique des technologies de l'information

1.3.16 Irrévocabilité : Propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

1.3.17 Mesure de sécurité : Moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'elles posent.

1.3.18 Renseignement de nature confidentielle : Renseignement qui ne doit pas être divulgué à des personnes non autorisées comme l'indiquent des dispositions de la Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels.

1.3.19 Renseignement personnel ou nominatif : Renseignement qui concerne une personne physique et qui permet de l'identifier.

1.3.20 Sécurité de l'information : Assurance, par un ensemble de mesures de sécurité, de rencontrer les objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'elles posent.

1.3.21 Système d'information : Système constitué de l'équipement, des procédures, des ressources humaines, ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information.

1.3.22 Technologie de l'information : Tout logiciel, matériel électronique ou combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, reproduire, protéger ou éliminer de l'information numérique.

1.3.23 Utilisateur : Toute personne de la Commission de quelque catégorie d'emploi, de statut d'employé ayant accès à l'actif informationnel, ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, accède à l'actif informationnel du ministère ou organisme.

2. CADRE LÉGISLATIF

- Loi sur l'instruction publique du Québec;
- Charte canadienne des droits et libertés;
- Loi sur les droits d'auteur;
- Charte québécoise des droits et libertés
- Code civil du Québec;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
- Loi sur les archives;
- Loi concernant le cadre juridique des technologies de l'information;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

3. ÉNONCÉS DE PRINCIPES GÉNÉRAUX

3.1 Protection des actifs informationnels

Cette politique de sécurité des actifs informationnels est fondée sur les énoncés généraux suivants :

- Les actifs informationnels de la Commission sont essentiels à ses opérations courantes et doivent faire l'objet d'une utilisation et d'une protection adéquates. Le niveau de protection accordé est fonction de leur sensibilité et des risques d'incidents, d'erreurs et de malveillance auxquels ils sont exposés.

- Les gestionnaires, particulièrement ceux qui sont désignés comme détenteurs d'actifs informationnels, sont les premiers responsables de la gestion de ces actifs, de leur utilisation par les employés et de l'application des mesures de contrôle nécessaire.

- La protection des actifs informationnels de la Commission s'appuie sur l'implication continue de tous les gestionnaires et de tous les utilisateurs.

- Chaque utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition en les utilisant avec discernement et aux seules fins prévues.

3.2 Signalement des incidents

Tout utilisateur a l'obligation de signaler sans tarder à son supérieur immédiat, lequel devra adresser la situation au directeur du Service des technologies de l'information, tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité tel que vol d'informations confidentielles, intrusion dans un réseau ou système, dommages délibérés, utilisation abusive, fraude, etc.

3.3 Droits de propriété intellectuelle

Les utilisateurs doivent se conformer aux exigences légales sur l'utilisation de produits à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle et sur l'utilisation de produits logiciels propriétaires.

3.4 Protection des renseignements confidentiels

Toute information considérée confidentielle ou sensible doit être protégée contre tout accès et toute utilisation non autorisés ou illicites. Sont notamment confidentiels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements nominatifs ainsi que tout renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

3.5 Continuité des activités de l'organisation

La Commission doit disposer de mesures d'urgence issues de son plan de continuité des services, consignées par écrit, éprouvées et mises à jour en vue d'assurer la remise en opération (dans un délai raisonnable) des systèmes d'information jugés essentiels en cas de sinistre majeur (ex. : incendie, attaque cybernétique, panne d'électricité prolongée, inondation, malveillance, etc.).

3.6 Sensibilisation et information

Chaque gestionnaire doit sensibiliser son personnel à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité ainsi qu'aux rôles et obligations de tous les employés de son unité administrative dans le processus de protection de ses actifs. Le gestionnaire doit également veiller à ce que le personnel soit informé sur les procédures de sécurité et sur l'utilisation correcte des actifs informationnels afin de minimiser les risques possibles.

3.7 Droit de regard

La Commission a un droit de regard sur l'utilisation de ses actifs informationnels par les utilisateurs. Les circonstances pour lesquelles ce droit de regard peut être exercé sont balisées par les lois pertinentes en vigueur.

4. RÔLES ET RESPONSABILITÉS

4.1 Le comité sur la sécurité de l'information numérique

Agit à titre de mécanisme de coordination et de concertation de la sécurité de l'information. Ce comité recommande les orientations et les directives à la direction générale et collabore avec la direction du Service des technologies de l'information à l'élaboration des standards, des pratiques et du plan d'action de sécurité des actifs informationnels de la Commission.

4.2 Le responsable de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

Veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels au sein de la Commission plus particulièrement dans le cadre du développement de systèmes d'information.

4.3 Le détenteur de l'information numérique

Agit à titre de responsable désigné de la protection d'un actif informationnel. À cet effet, il :

- Assure la gestion de la sécurité de son actif informationnel.
- Veille à ce que les mesures de sécurité appropriées soient élaborées, mises en place et appliquées.
- Participe à la sensibilisation des utilisateurs aux besoins de sécurité de l'information qu'ils manipulent.
- Répond de l'utilisation, par les utilisateurs et les partenaires de la Commission, des données dont il est le détenteur. À cet égard, il voit à élaborer un protocole d'entente avec les entités utilisatrices et à la faire respecter.

4.4 Le gestionnaire

Les principales responsabilités du gestionnaire à l'égard de la protection des actifs informationnels sont, entre autres :

- D'informer et sensibiliser son personnel quant aux dispositions de la présente politique et des modalités liées à sa mise en œuvre.

- De s'assurer que les ressources informationnelles sont utilisées en conformité avec les principes généraux et les autres exigences de la présente politique.

- De répondre de l'utilisation faite par son personnel des actifs informationnels de la Commission.

4.5 L'utilisateur

L'utilisateur d'un actif informationnel :

- Prend connaissance de la politique de sécurité des actifs informationnels.

- Utilise les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont autorisés.

- Se conforme aux consignes et aux directives établies et dans le respect des dispositions de la présente politique.

4.6 La direction du Service des technologies de l'information

Assure la mise en application des exigences de sécurité des actifs informationnels de la Commission durant tout le cycle de vie de l'information numérique. Ses principales responsabilités sont, entre autres :

- D'assurer la sécurité des actifs informationnels de la Commission.

- D'assurer la disponibilité, l'intégrité, la confidentialité, l'authentification, l'irrévocabilité de l'information numérique selon les exigences et les droits d'accès définis par les détenteurs des actifs informationnels.

- De fournir aux détenteurs le soutien, les conseils, dont les standards de sécurité, en matière de protection de leurs actifs informationnels.

- De restreindre les accès de son personnel spécialisé en technologies de l'information, notamment les administrateurs de réseaux, aux seules informations indispensables à l'exercice de leurs fonctions.

5. POLITIQUE RELATIVE À L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION

Toute utilisation des actifs informationnels est soumise à la politique d'utilisation des technologies de l'information.

6. RÈGLES D'ACCÈS AUX ACTIFS INFORMATIONNELS

6.1 Identification et authentification des utilisateurs

Tout utilisateur désirant accéder aux actifs informationnels de la Commission doit préalablement s'identifier et s'authentifier à l'aide d'un identifiant ou code d'utilisateur et d'un mot de passe. Seules les personnes dûment autorisées et possédant un droit d'utilisation peuvent y accéder. Les identifiants et les mots de passe sont confidentiels et ne doivent en aucun temps être divulgués. Toute action commise sous ces authentifications est présumée être du ressort de l'utilisateur concerné.

Tout système d'information que la Commission désire protéger doit contenir un processus d'accès nécessitant un mécanisme d'identification et d'authentification de l'utilisateur. Le mécanisme doit limiter cet accès uniquement aux personnes dûment autorisées en fonction du

niveau d'autorisation que ces dernières détiennent et de la nature de l'information et des applications utilisées.

6.2 Accès

Tout accès ou tentative d'accès non autorisé aux actifs informationnels de la Commission constitue une violation de la présente politique.

7. GESTION DE L'INFORMATION

7.1 Confidentialité

L'information issue de tout média de conservation de données des actifs informationnels de la Commission est confidentielle, si elle a le caractère d'un renseignement nominatif ou d'un renseignement que la Commission peut ou doit protéger en vertu d'une législation, d'un règlement, d'un contrat ou d'une entente de confidentialité.

Personne n'est autorisé à transmettre ou divulguer à des tiers une information considérée comme confidentielle par la Commission ou une législation, sauf lorsque la personne visée par cette information le permet spécifiquement, lorsque le destinataire est lui-même une personne autorisée ou lorsque prescrit par une législation.

Le droit de l'utilisateur à la confidentialité de l'information qui lui est propre ne s'étend pas dans l'éventualité où il fait usage d'actifs informationnels de façon contraire à la présente politique, à la politique relative à l'utilisation des technologies de l'information, aux lois ou aux normes de la Commission.

L'utilisateur qui extrait des données des actifs informationnels pour constituer des fichiers informatisés aux fins du déroulement de toute activité est soumis aux règles de la présente politique.

7.2 Intégrité

Les gestionnaires et les utilisateurs doivent protéger les informations qu'ils détiennent en fonction des risques liés à leur environnement, soit dans le cadre de leurs fonctions à titre de membre du personnel, soit dans le cadre d'une entente formelle avec la Commission à titre de client ou fournisseur, soit privément à titre personnel, et s'il y a lieu, en protéger l'accès par un mot de passe ou autre mesure de sécurité appropriée.

7.3 Disposition de l'information

Tout extrait issu d'actifs informationnels contenant de l'information confidentielle doit être conservé de façon sécuritaire, et détruit selon les normes de sécurité, de confidentialité, et éventuellement de conservation des documents prescrite par le Service du secrétariat général et des communications.

Tout ordinateur dont on veut se départir doit faire l'objet d'un examen avant qu'il ne soit remis à son nouveau destinataire ou envoyé au recyclage ou aux rebuts. L'information, les programmes et les logiciels contenus sur les disques rigides ou dans la mémoire des équipements dont on veut se défaire doivent être détruits ou enlevés. Cette responsabilité relève du Service des technologies de l'information.

8. MESURES DE SÉCURITÉ ET D'URGENCE

8.1 Vérifications

Des vérifications périodiques peuvent être effectuées à l'initiative du directeur du Service des technologies de l'information pour évaluer de façon préventive les niveaux de risque potentiels ou de façon corrective si des vulnérabilités sont identifiées.

Sauf circonstances exceptionnelles, une vérification technique des actifs informationnels, qui nécessiterait la lecture des informations personnelles et privées d'un utilisateur, ne peut être effectuée que par des personnes autorisées, dans le cadre de leurs fonctions, après avoir prévenu la personne concernée lorsque cela est possible.

8.2 Plan de relève et de continuité des services

Des mesures d'urgence doivent être prises par les détenteurs d'actifs informationnels conjointement avec le Service des technologies de l'information, consignées par écrit et éprouvées, pour assurer la remise en opération des actifs informationnels et de télécommunications institutionnelles considérées comme essentielles en cas de force majeure.

9. DISPOSITIONS FINALES

9.1 Sanctions

Lorsqu'un utilisateur d'actif informationnel contrevient à cette politique ou aux normes internes en découlant, l'autorité administrative responsable détermine, selon la nature ou la gravité du cas, de l'opportunité d'appliquer une sanction disciplinaire ou une mesure administrative, conformément aux dispositions des conventions collectives, ententes et règlements. La révocation de l'utilisation d'actifs informationnels peut également être effectuée.

L'autorité administrative responsable peut aussi référer à toute autre autorité judiciaire les informations colligées et qui la portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise. La direction générale de la Commission doit préalablement être informée de la situation et de la démarche envisagée.

9.2 Révision

Afin d'assurer son adéquation aux besoins de la Commission et des changements technologiques, la présente politique doit être régulièrement révisée dans une fenêtre de trois à cinq ans après sa mise en application ainsi que lors de changements qui pourraient l'affecter.

9.3 Directives du ministère de l'Éducation, du Loisir et du Sport (MELS)

Toute directive du MELS relative à la sécurité des actifs informationnels devra être implantée au sein de la Commission dans les meilleurs délais et la présente politique devra être modifiée si nécessaire.

9.4 Mise en application et suivi de la politique

La direction du Service des technologies de l'information est chargée de l'application de la présente politique.

9.5 Date d'entrée en vigueur

La présente politique entre en vigueur à la date de son adoption par le conseil des commissaires.