Référer à la :
POL 06-05

SECTION I – PRÉAMBULE

Préambule

1. La *Politique sur la sécurité de l'information* (ci-après appelée la « présente politique ») prévoit ce qui suit :

Définitions

2. On entend par :

2.1 **Actif informationnel** : Une information numérique, une banque d'information numérique, un système ou un support d'information, une documentation, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par l'École nationale de police du Québec (ci-après appelée l'« École »);

2.2 **Analyse et évaluation des risques :** Analyse et évaluation des menaces, des impacts et des vulnérabilités auxquels l'information et les infrastructures de traitement de l'information sont exposées et de la probabilité de leur survenance;

2.3 **Application :** Ensemble organisé de moyens informatiques (traitements, données et interfaces), incluant les progiciels mis en place pour recueillir, traiter, emmagasiner, communiquer et éliminer l'information dans le but de répondre à un besoin déterminé et de supporter les processus de travail des utilisateurs;

2.4 **Audit :** Évaluation périodique basée sur des critères définis permettant de vérifier le degré de conformité;

2.5 **Authentification :** Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif lors d'un échange électronique;

2.6 **Autorisation :** Attribution, par une autorité, de droits d'accès aux actifs informationnels qui consiste en un privilège d'accès accordé à une personne, à un dispositif ou à une entité;

2.7 **Banque d'information :** Ensemble d'information relative à un domaine défini, regroupée et organisée de façon à en permettre l'accès;

2.8 **CAIPRPSI** : Comité sur l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information;

2.9 **Catégorisation :** Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles caractérisent le degré de sensibilité de cette information et, conséquemment, de la protection à lui accorder;

2.10 **Chiffrement :** Opération par laquelle un texte en clair est substitué à un texte inintelligible, inexploitable pour quiconque ne possédant pas la clé permettant de le ramener à sa forme initiale;

2.11 **Clé :** Paramètre constitué d'une séquence de symboles et utilisé avec un algorithme cryptographique pour transformer, valider, authentifier, chiffrer ou déchiffrer des données;

2.12 **Confidentialité :** Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes désignées et autorisées par l'École;

2.13 **Cycle de vie de l'information :** Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction en conformité avec le calendrier des délais de conservation de l'École;

2.14 **Détenteur d'actif informationnel :** Cadre à qui est assignée la responsabilité de la sécurité d'un actif informationnel;

2.15 **DIC** : Catégorisation des actifs informationnels par l'assignation d'une valeur en termes de Disponibilité, d'Intégrité et de Confidentialité;

2.16 Directive : Ensemble de règles de conduite sur un sujet;

2.17 Document : Ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ses formes ou en un autre système de symboles. Est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite;

2.18 Droit d'auteur : Droit exclusif de reproduire une source créatrice ou de permettre à une autre personne de le faire. Il comprend le droit exclusif de publier, de produire, de reproduire, d'exécuter en public, de traduire, de communiquer au public par des moyens de télécommunications, d'exposer une œuvre artistique à certaines conditions, et dans certains cas, de louer une œuvre;

2.19 Équipement informatique : Ordinateur, mini-ordinateur, micro-ordinateur, poste de travail informatisé et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information, et tout équipement de télécommunications;

2.20 Fournisseur : Personne morale ou physique ou société ayant des activités professionnelles d'ordre commercial ou industriel, de formation ou de services-conseils;

2.21 Identification : Fonction du contrôle de l'accès aux actifs informationnels permettant d'attribuer un code d'identification à un utilisateur, à un dispositif ou à une autre entité afin de l'identifier;

2.22 Incident de sécurité : Circonstance au cours de laquelle la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel a été affectée de même que toute situation présentant les conditions requises pour potentiellement produire un tel résultat;

2.23 **Information :** Élément de connaissance concernant un phénomène et qui, pris dans un contexte déterminé, a une signification particulière;

2.24 **Information électronique :** Information sous toute forme (textuelle, symbolique, sonore ou visuelle) dont l'accès et l'utilisation ne sont possibles qu'au moyen des technologies de l'information;

2.25 **Intégrité :** Information contenue dans un document qui n'est pas altérée et qui est maintenue dans son intégralité et que le support qui porte cette information lui procure la stabilité et la pérennité voulue;

2.26 **Logiciel :** Ensemble de programme, de procédure et de règle, ainsi que de la documentation qui leur est associée, nécessaires à la mise en œuvre d'un système de traitement de l'information;

2.27 **Mécanisme 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'ils posent;

2.28 **Médias sociaux :** Média numérique basé sur les technologies du Web 2.0, qui vise à faciliter la création et le partage de contenu généré par les utilisateurs, la collaboration et l'interaction sociale;

2.29 **Mot de passe :** Authentifiant prenant la forme d'une chaîne de caractères alphanumériques, généralement choisie par l'utilisateur, que celui-ci doit entrer lors de la procédure d'accès à un système informatique, notamment à un réseau ou à sa boîte aux lettres électronique;

2.30 **Norme :** Accord documenté contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi. Le terme « norme » accompagné du qualificatif « internationale », « nationale » ou « européenne » signifie une norme reconnue par un organisme officiel;

2.31 **Personne :** Personne physique ou morale;

2.32 Personnel : Ensemble des ressources humaines, rémunérées ou non, de l'École;

2.33 Pratique : Savoir ou manière de faire qui conduisent au résultat souhaité et qui sont portés en exemple auprès des pairs afin de leur faire partager l'expérience qui leur permettra une amélioration collective;

2.34 Procédure : Ensemble des actes à accomplir afin d'obtenir une décision administrative;

2.35 Progiciel : Logiciel d'application paramétrables, destiné à la réalisation de diverses tâches;

2.36 Renseignement personnel : Renseignement qui concerne une personne physique et qui permet de l'identifier;

2.37 Réseau : Ensemble d'équipements qui sont reliés les uns aux autres par des câbles ou des faisceaux hertziens, afin qu'ils puissent échanger, distribuer ou diffuser des informations et partager différentes ressources;

2.38 Ressources informationnelles : Ensemble de ressources qui peuvent être répertoriées dans l'actif informationnel de l'École. Une ressource informationnelle peut être une ressource humaine, matérielle ou financière directement affectée à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information;

2.39 Sécurité de l'information : Protection des ressources informationnelles de l'École, face à des risques identifiés, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée;

2.40 Standard : Norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation comme l'ISO, le CCN, etc., mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'organisations ou encore d'un consortium;

2.41 Système d'information : Ensemble de tous les éléments qui contribuent au traitement et à la circulation de l'information dans l'École (base de données,

logiciels d'application, procédures, documentation, etc.) y compris le système informatique proprement dit (unité centrale de traitement, périphériques, système d'exploitation, etc.);

2.42 **Technologie de l'information :** Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visible). Une technologie de l'information peut être électronique, magnétique, optique, sans fil ou autres;

2.43 **Télécommunication :** Transmission à distance de signaux porteurs d'information qui s'effectue au moyen de câbles ou d'ondes électromagnétiques;

2.44 **Utilisateur :** Un membre du personnel de l'École, un contractant, un étudiant ou un client ayant accès à l'actif informationnel de l'École;

2.45 **Utilisation :** Terme qui recouvre, le cas échéant, l'ensemble des événements constituant le cycle de vie de l'information électronique dont, entre autres, la création, la collecte, le traitement, la conservation, l'interrogation, la communication, la modification, l'archivage et la destruction;

2.46 **Virus :** Programme malveillant dont l'exécution est déclenchée lorsque le vecteur auquel il a été attaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des zones systèmes lui servant à leur tour de moyen de propagation, et qui produit les actions malveillantes pour lesquelles il a été conçu.

Objets

3. La présente politique a pour objet :

3.1 d'assurer le respect de toute législation relative à la sécurité de l'information, et ce, tout au long du cycle de vie d'un actif informationnel;

3.2 d'assurer la cohérence et la coordination des différents intervenants de l'École en matière de sécurité de l'information et d'établir leurs rôles et responsabilités;

3.3 d'établir les règles régissant l'utilisation des actifs informationnels à l'École.

Champ d'application

4. La présente politique s'applique à tous les utilisateurs d'actifs informationnels de l'École.

SECTION II – DISPOSITIONS GÉNÉRALES

Principes directeurs

5. Les principes directeurs de la présente politique sont les suivants :

5.1 Respect de la législation applicable :

Aux fins de l'article 3.1, la présente politique vise à respecter, notamment, les lois suivantes : *Charte canadienne des droits et libertés* (1982, c. 11), *Code criminel* (L.R. (1985), c. C-46), *Loi sur le droit d'auteur* (L.R. (1985), c. C-42), *Loi sur les marques de commerce* (L.R. (1985), c. T-13), *Charte des droits et libertés de la personne* (L.R.Q., c. C-12), *Code civil du Québec* (L.Q., 1991 c. 64), *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1), *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1) et la *Loi sur les archives* (L.R.Q., c. A-21.1).

5.2 Principes généraux :

Tout utilisateur assume des responsabilités spécifiques en matière de sécurité de l'information et est responsable de ses actions.

Les mesures de protection, de prévention, de détection, d'assurance et de correction doivent permettre d'assurer la confidentialité, l'intégrité, la disponibilité, l'authentification et l'irrévocabilité des actifs informationnels. Elles doivent, notamment, empêcher les accidents, l'erreur, la malveillance ou la destruction d'information.

Les engagements contractuels dont l'École est partie prenante doivent, lorsque nécessaire, contenir des dispositions garantissant le respect des exigences en matière de sécurité et de protection de l'information, et ce, notamment, par l'ajout d'une clause d'engagement de confidentialité.

5.3 Protection de l'information et des actifs informationnels :

Les actifs informationnels de l'École sont essentiels à ses opérations courantes et doivent faire l'objet d'une utilisation et d'une protection adéquate.

Les actifs informationnels doivent faire l'objet d'une identification, d'une catégorisation et d'une classification, et ce, en collaboration avec les détenteurs d'actif informationnel.

Les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger et sont établies en fonction des risques et de leurs impacts. Elles doivent également assurer l'accessibilité de l'information en temps voulu et de limiter sa divulgation aux seules personnes intéressées ainsi que d'assurer son intégrité.

La gestion de la sécurité de l'information doit être incluse et appliquée tout au long du cycle de vie d'un actif informationnel.

5.4 Signalement d'un incident de sécurité :

Un utilisateur a l'obligation de signaler sans tarder à une personne en autorité de l'École tout acte susceptible de représenter une violation réelle ou présumée des actifs informationnels.

5.5 Propriété intellectuelle :

Un utilisateur est assujetti à la *Politique sur la propriété intellectuelle de l'École nationale de police du Québec* (POL 04-02).

5.6 Protection des renseignements personnels et confidentiels :

Toute information considérée confidentielle doit être protégée contre tout accès

ou utilisation non autorisés ou illicites.

Les renseignements personnels ne peuvent être utilisés qu'aux fins pour lesquels ils ont été recueillis ou obtenus.

Chaque système informationnel doit prévoir des droits d'accès différents selon les catégories d'utilisateurs.

5.7 Continuité des activités de l'École :

L'École doit disposer de mesures d'urgence issues de son plan de continuité et de relève des services, consignées par écrit, éprouvées et mises à jour en vue d'assurer la remise en opération dans un délai raisonnable des actifs informationnels jugés essentiels en cas de sinistre majeur (ex. : incendie, panne électrique prolongée, inondation, malveillance, etc.).

5.8 Sensibilisation et information :

Un cadre doit sensibiliser et informer son personnel au niveau de la sécurité des actifs informationnels de l'École ainsi qu'au rôle et obligations de chaque employé dans les processus et procédures de protection, de sécurité et d'utilisation de ses actifs.

5.9 Droit de regard :

Comme les actifs informationnels appartiennent à l'École, celle-ci a un droit de regard sur l'utilisation qui en est faite par un utilisateur. Les circonstances pour lesquelles ce droit de regard peut être exercé doivent être clairement définies et diffusées auprès des utilisateurs, et ce, par un message d'accueil sur la confidentialité lors du démarrage d'un équipement informatique de l'École.

5.10 Éthique :

Un utilisateur est assujetti à la *Directive sur l'éthique à l'École nationale de police du Québec* (DIR 05-04).

Rôles et responsabilités des divers intervenants :

6. Les rôles et responsabilités des intervenants sont les suivants :

6.1 Le directeur général de l'École :

Le directeur général est le premier responsable de la sécurité des actifs informationnels de l'École. A ce titre, il doit :

- s'assurer de la mise en œuvre des responsabilités et des obligations attribuées par la présente politique;
- désigner le responsable de la sécurité de l'information à l'École;
- présider le Comité sur l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information et y nommer les membres;

Il soumet un bilan annuel dans le rapport annuel de gestion de l'École.

6.2 Le responsable de la sécurité de l'information :

À titre de représentant désigné par le directeur général en matière de sécurité de l'information, le responsable de la sécurité de l'information gère et coordonne la sécurité de l'information au sein de l'École. Il doit, notamment, élaborer, mettre en place, effectuer le suivi et l'évaluation de la sécurité de l'information. À cet effet, il a les responsabilités suivantes :

- coordonner la mise en oeuvre de la présente politique;
- veiller au respect de la présente politique;
- élaborer les directives, procédures et autres documents administratifs découlant de la mise en œuvre de la présente politique;
- proposer les orientations de sécurité de l'information et les communiquer aux utilisateurs des actifs informationnels de l'École;

- identifier, en collaboration avec les cadres, les détenteurs d'actif informationnel dans leur unité administrative;

- participer aux réunions du Comité sur l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information;

- s'informer des besoins en matière de sécurité auprès des détenteurs d'actif informationnel et cadres, de leur proposer des solutions et de coordonner la mise en place de ces solutions;

- suivre la mise en oeuvre de toute recommandation découlant d'une vérification ou d'un audit;

- gérer les aspects relatifs à l'escalade des incidents de sécurité et procéder à l'évaluation de la situation en matière de sécurité.

6.3 Le responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP) :

A titre de responsable de l'application de la *Loi sur l'accès aux documents des établissements organismes publics et sur la protection des renseignements personnels,* le RAIPRP doit s'assurer que les mécanismes de sécurité mis en place respectent la législation mentionnée à l'article 5.1 de la présente politique.

Il doit également conseiller le responsable de la sécurité de l'information lors de l'acquisition ou le développement d'un nouveau système d'information.

6.4 Le cadre :

Le cadre à l'égard de la protection des actifs informationnels :

- s'assure que le personnel relevant de son autorité est au fait de leurs obligations découlant de la présente politique;

- informe et sensibilise le personnel relevant de son autorité de l'importance des enjeux de la sécurité de l'information, et ce, conformément à l'article 5.8 de la présente politique;

- s'assure que les informations et les ressources de l'École sont utilisées en conformité avec les principes directeurs et autres exigences de la présente politique;

- communique au responsable de la sécurité de l'information tout problème d'importance en matière de sécurité de l'information.

6.5 Le détenteur d'actif informationnel :

- assure la sécurité d'un ou de plusieurs actifs informationnels confiés par une personne autorisée de l'École;

- s'implique dans l'ensemble des activités relatives à la sécurité afin de préserver notamment l'intégrité de l'information par l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non infomatiques et finalement la prise en charge des risques résiduels;

- veille à ce que les mesures de sécurité appropriées soient élaborées, mises en places et appliquées;

- détermine les règles d'accès aux actifs informationnels dont ils assument la responsabilité en collaboration avec le responsable de la sécurité de l'information;

- participe à la sensibilisation des utilisateurs.

6.6 Le personnel relevant du Service des ressources matérielles et des technologies de l'information

Le personnel relevant du Service des ressources matérielles et des technologies de l'information assure la mise en application des exigences de sécurité des actifs informationnels de l'École. Il coordonne les travaux reliés à l'implantation des travaux techniques de la sécurité et réalise les tâches de sécurité opérationnelles qui lui sont confiées par le responsable de la sécurité de l'information.

Les principales responsabilités du personnel de cette unité administrative sont de :

- fournir aux détenteurs d'actif informationnel le soutien et les conseils en matière de sécurité de l'information;
- assurer la sécurité des actifs informationnels relevant de sa responsabilité;
- assurer la disponibilité, l'intégrité, la confidentialité selon les exigences définies par les détenteurs d'actif informationnel;
- Selon les directives du responsable de sécurité de l'information, il restreint les accès de son personnel spécialisé en technologies de l'information aux seules informations indispensables à l'exercice de leurs fonctions.

6.7 L'utilisateur :

Un utilisateur doit respecter la présente politique, les normes, standards, directives, procédures et autres documents administratifs en vigueur en matière de sécurité de l'information. Plus particulièrement, il doit :

- prendre connaissance et adhérer à la présente politique;
- utiliser les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont autorisés;
- informer une personne en autorité de l'École de toute violation des mesures de sécurité dont il pourrait être témoin ou de toute anomalie décelée pouvant nuire à la protection de l'information.

6.8 Le personnel relevant de la Direction des ressources humaines :

Le personnel relevant de la Direction des ressources humaines est responsable d'informer tout nouvel employé ou utilisateur contractuel recommandé par cette direction de ses obligations en vertu de la présente politique ainsi que des normes, standards, directives, procédures et autres documents administratifs qui en découlent.

Le personnel de cette direction doit également s'assurer de l'engagement de cet employé ou de l'utilisateur contractuel à respecter la présente politique, les normes, standards, directives, procédures et autres documents administratifs qui en découlent.

6.9 Comité sur l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information (comité).

Le comité constitue un mécanisme de coordination et de concertation afin de proposer des orientations et de faire des recommandations en regard de l'élaboration, la mise en œuvre et la mise à jour de la présente politique ainsi que des directives qui en découlent. De plus, le comité doit respecter les obligations qui lui sont attribuées dans le règlement adopté en vertu de l'article 63.2 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Sanction, mesure administrative ou disciplinaire

7. Lorsqu'un utilisateur contrevient à la présente politique, aux directives, procédures ou autres documents administratifs qui en découlent, une personne en autorité de l'École détermine, selon la nature ou la gravité du cas, de l'opportunité d'appliquer une sanction, mesure administrative ou disciplinaire.

La direction de l'École peut également référer toute violation à une autorité policière ou judiciaire compétente.

Responsable

8. Le directeur du soutien administratif et technologique est responsable de l'application et de la mise à jour de la présente politique.

Remplacement

9. La présente politique remplace la politique du 19 décembre 2006.

Article final

10. La POL 06-05 comprend 10 articles.

La directrice générale,

Original signé

_____

Marie Gagnon