CÉGEP SHAWINIGAN
Du savoir et des gens

POLITIQUE
La sécurité de l'information

3

Direction générale

Première approbation	Dernière mise à jour	Abrogation	Prochaine révision
	2024-06-11 | CA/2024-539-8.2		2028-2029

Table des matières

RÉFÉRENCES

- *La Directive gouvernementale sur la sécurité de l'information*
- *Le Cadre gouvernemental de gestion de la sécurité de l'information*
- *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)*
- *La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25)*
- *Le Règlement sur les incidents de confidentialité*
- *La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03)*
- *La Loi sur les archives (LRQ, chapitre A-21.1)*
- *Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2)*
- *Le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information*
- *Le cadre gouvernemental de gestion de la sécurité de l'information*
- *Les pratiques gouvernementales en matière de sécurité de l'information*

PRÉAMBULE

Le Cégep de Shawinigan reconnaît que l'information et les technologies qui la supportent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission d'enseignement et de recherche et, vu la valeur administrative, légale et financière de ses actifs informationnels, ils doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriées et adéquates tout au long de leur cycle de vie, selon les bonnes pratiques en la matière de sécurité informationnelle et avec une approche de gestion des risques, quel qu'en soit le support ou l'emplacement.

L'application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre. G-1.03), de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25), et de la *Directive gouvernementale sur la sécurité de l'information* (2021) du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics, impose des obligations importantes aux établissements collégiaux.

Pour se conformer et répondre à ses obligations réglementaires et légales, le Cégep de Shawinigan doit adopter, garder à jour et veiller à l'application d'une politique de sécurité de l'information (SI) pour assurer la mise en place des processus formels de la sécurité de l'information afin d'encadrer la gestion des risques, la gestion des accès aux actifs informationnels, la gestion des incidents et la gestion de la continuité des activités.

Dans le cadre de la révision la *Politique 3 de la sécurité de l'information* au cours de la session Hiver 2024, la Direction abroge la *Politique 24 sur l'utilisation des équipements et réseaux informatiques et de télécommunications* pour l'intégrer dans la présente politique.

ARTICLE 1 – CADRE LÉGAL

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales. Pour plus de précisions, voir la section *Références*.

ARTICLE 2 - DÉFINITIONS

2.1. Actif informationnel

Information numérique, document numérique, système d'information, documentation, équipement informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitué par le Cégep pour mener à bien sa mission.

2.2. Code d'accès

Mécanisme d'identification et d'authentification par un code individuel et un mot de passe ou de ce qui en tient lieu, notamment une carte magnétique ou carte à puce, servant à identifier de façon unique un utilisateur qui utilise un actif informationnel du Cégep.

2.3. Cycle de vie de l'information

L'ensemble des étapes que parcourt une information, 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 de conservation du Cégep.

2.4. Équipement informatique

Ordinateurs, mini-ordinateurs, postes de travail informatisés 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.

2.5. Plan de relève informatique

Ensemble de procédures qui décrivent de façon précise les mesures à suivre pour remettre en état de fonctionnement un système informatique à la suite d'une panne ou un sinistre majeur.

2.6. Technologies de l'information

Regroupent les systèmes et les processus, principalement de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information.

ARTICLE 3 – OBJECTIFS

La présente politique constitue le cadre général qui vise la gestion des actifs informationnels dans le respect des droits et obligations du Cégep en cette matière pour garantir et répondre aux objectifs de sécurité de l'information et plus spécifiquement pour :

- assurer la protection de l'actif informationnel tout au long de son cycle de vie, quel que soit le support ou l'emplacement;
- assurer la disponibilité de l'information pour qu'elle soit accessible au moment voulu et utilisable à la demande par l'entité autorisée;
- assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon sans autorisation;
- préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou la divulguer à des personnes, entités ou processus non autorisés;
- regrouper les lignes directrices et les rôles et responsabilités des intervenants en sécurité;

- identifier et classifier les actifs informationnels du Cégep selon leurs degrés de criticité et veiller constamment à leur évaluation ainsi que leur protection adéquate;
- assurer la conformité aux lois et cadres réglementaires;
- mettre en place un plan de continuité des activités et de relève informatique;
- assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements personnels.

ARTICLE 4 – ÉNONCÉ DES PRINCIPES GÉNÉRAUX

4.1. Protection de l'information

La sécurité de l'information s'articule autour des trois principes suivants :

4.1.1. Disponibilité

La disponibilité garantit que les utilisateurs autorisés d'un système ont un accès opportun et ininterrompu aux informations contenues dans ce système, ainsi qu'au réseau. Les informations doivent être accessibles en temps utile et de la manière requise par un utilisateur autorisé. Afin d'aider à assurer cette disponibilité, des mesures de contrôles doivent être mises en place.

4.1.2. Intégrité

L'intégrité des données consiste à garantir que les données n'ont pas été modifiées d'aucune façon au cours de leur communication, qu'il s'agisse de données au repos, en transit ou en mémoire. Afin d'assurer l'intégrité des données, des mesures de sécurité physiques et d'accès logiques doivent être mises en place.

4.1.3. Confidentialité

La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles et des renseignements personnels. Elle a pour but de s'assurer qu'une information ou une donnée soit accessible uniquement par les personnes autorisées. La confidentialité de l'information doit aussi être assurée tout au long de son cycle de vie. Afin de garantir la confidentialité, des mesures de contrôle doivent être mises en place.

4.2. Catégorisation de l'information

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie. Pour cette raison il est primordial de garder à jour l'inventaire de l'ensemble des actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des actifs informationnels d'une organisation. La catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des actifs dans le but d'en déterminer le niveau de protection.

Il est important de réévaluer la catégorisation des actifs informationnels sur une base périodique pour s'assurer que la catégorisation attribuée est toujours appropriée en fonction des modifications des obligations légales et contractuelles, ainsi que des changements dans l'utilisation des données ou leur valeur pour l'établissement. Cette évaluation devrait être effectuée par le responsable de l'actif informationnel.

ARTICLE 5 – CHAMP D'APPLICATION

5.1. Personnes visées

Cette politique vise sans exception l'ensemble des personnes physiques et morales, régulières ou occasionnelles, peu importe leur statut, appelées à utiliser les actifs informationnels du Cégep citant, entre autres :

- le personnel à l'emploi du Cégep;
- les étudiantes et étudiants du Cégep;
- les partenaires, fournisseurs, contractants et tiers du Cégep.

5.2. Actifs visés

La politique vise aussi toutes les informations et les actifs informationnels :

- appartenant au Cégep;
- détenus par un tiers, mais appartenant au Cégep;
- utilisés et détenus par un tiers au bénéfice ou au nom du Cégep;
- et ce, quel que soit le support de conservation (électronique, technologique, papier, etc.).

5.3. Activités visées

Cette politique concerne l'ensemble des activités entrant dans le cycle de vie de l'information, à savoir : la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des actifs informationnels du Cégep, qu'elles soient conduites dans le périmètre de ses locaux, dans un autre endroit ou à distance.

ARTICLE 6 – CADRE DE GESTION

La mise en œuvre de la présente politique s'appuie sur la définition d'un cadre de gestion en sécurité de l'information qui précise le champ d'action des différents intervenants. Le cadre de gestion précise l'organisation fonctionnelle en matière de sécurité de l'information et rend possibles la définition d'objectifs clairs et une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des risques et des menaces.

La politique de sécurité de l'information du Cégep se base sur cinq axes fondamentaux de gestion.

6.1. Gestion des identités et des accès (GIA)

La gestion des identités et des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le Cégep soient strictement réservés aux personnes autorisées afin de protéger la confidentialité.

6.2. Gestion des vulnérabilités

La gestion des vulnérabilités se caractérise par un déploiement des mesures pour maintenir à jour les logiciels du parc informatique, afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une gestion de notification des vulnérabilités venant des fournisseurs ou des prestataires de services doit être en place pour qu'elles soient évaluées et corrigées, le cas échéant.

6.3. Gestion du risque

La gestion des risques touchant l'actif informationnel du Cégep est basée sur une analyse des menaces encourues reliées à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le Cégep. De cette analyse découlent des directives reliées à l'utilisation et l'opération des systèmes d'information ainsi qu'aux résultats escomptés.

6.4. Gestion des incidents

La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relativement aux incidents de sécurité et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services. Dans la gestion des incidents, le Cégep peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

6.5. Gestion de la reprise et de la continuité des affaires

La gestion de la reprise et de la continuité des affaires se caractérise par la mise en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer l'institution financière tels les catastrophes naturelles, les pannes d'électricité ou de télécommunication, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités de l'institution et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

ARTICLE 7 – RÔLES ET RESPONSABILITÉS

La présente politique attribue la gestion de la sécurité de l'information du Cégep à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

7.1. Direction générale

La Direction générale avec l'aide de la personne cheffe de la sécurité adopte les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information. Elle assume aussi le processus de délégation des rôles de chef(fe) de la sécurité de l'information organisationnelle (CSIO) et de coordination organisationnelle des mesures de sécurité de l'information (COMSI).

7.2. Responsable de la protection des renseignements personnels – Responsable du registrariat

La personne responsable de la protection des renseignements personnels veille à assurer le respect et la mise en œuvre de la *Loi sur la protection des renseignements personnels* afin de mettre en œuvre des politiques et pratiques encadrant la gouvernance des renseignements personnels.

7.3. Cheffe ou chef de la sécurité de l'information organisationnelle (CSIO) – Coordonnateur informatique

La personne assumant la fonction de CSIO est un membre du personnel d'encadrement d'un organisme public. Cette personne assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. La ou le CSIO est responsable de la diffusion et de la mise en application de la politique. Cette fonction est assurée par la coordination informatique.

7.4. Coordonnatrice ou coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

La personne assumant la fonction de COMSI est un membre du personnel professionnel ou cadre qui agit sur le plan opérationnel. Elle intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire au CSIO de l'établissement, notamment en matière de la gestion des incidents et des risques en sécurité de l'information.

La ou le COMSI représente l'organisme public auprès du Réseau d'alerte gouvernemental. Cette personne est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) dans son cégep, en soutien à la personne cheffe de la sécurité de l'information organisationnelle (CSIO).

Elle collabore auprès du CSIO du Cégep à l'élaboration des divers éléments stratégiques et tactiques en sécurité informationnelle :

- elle maintient le registre des événements et des incidents liés à la sécurité de l'information;
- elle effectue et participe aux analyses de risques en sécurité de l'information;
- elle gère le processus de gestion, de déclaration des incidents et de résolution de problème et contribue à sa mise en place;
- elle contribue au processus formel de gestion des droits d'accès à l'information.

7.5. Coordination des technologies de l'information - Coordonnateur informatique

La coordination des technologies de l'information assume la responsabilité de l'application de la présente politique. Elle s'assure de la prise en charge des exigences de SI dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information. Cette fonction est assurée par la personne à la coordination informatique.

7.6. Direction des ressources humaines et du secrétariat général

En matière de sécurité de l'information, la direction des ressources humaines et du secrétariat général doit :

- vérifier, au besoin, les antécédents des personnes candidates à l'embauche et des membres du personnel impliqués dans la sécurité de l'information;
- s'assurer que les responsabilités des intervenants concernant la sécurité de l'information et le respect de la présente politique, ainsi que du cadre normatif des ressources informationnelles, sont inscrites dans les descriptions de tâches des membres du personnel;
- informer et obtenir de tout nouvel employé du Cégep son engagement au respect de la présente politique;
- imposer les sanctions appropriées lors de violation des politiques, règlements, directives et code de conduite touchant à la sécurité de l'information.

7.7. Responsable d'actifs informationnels

La personne assumant le rôle de responsable d'actifs informationnels est la personne-cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il ou elle :

- participe à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de risques;
- veille à la protection de l'information et des systèmes d'information en conformité avec la politique de la SI;
- rapporte tout événement ou toute menace liée à la SI;
- collabore à la mise en œuvre de toute mesure pour améliorer la SI afin de remédier à un incident au besoin.

7.8. Utilisatrices et utilisateurs

La responsabilité de la sécurité de l'information du Cégep incombe à toutes les utilisatrices et à tous les utilisateurs des actifs informationnels du Cégep. Tout utilisatrice ou utilisateur qui accède à une information, qui la consulte ou qui la traite, est responsable de l'utilisation qu'il ou elle en fait et doit procéder de manière à protéger cette information.

À cette fin, l'utilisatrice ou l'utilisateur doit :

- se conformer à la présente politique et à toute autre directive du Cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- être responsable des actions résultant de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu'il démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;
- aviser une personne responsable, un membre du personnel enseignant ou son supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel;
- au besoin, participer à la catégorisation de l'information de son service;
- utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre approprié à son utilisation et aux fins auxquelles ils sont destinés;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou un incident de sécurité de l'information.

ARTICLE 8 – FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption des comportements sécuritaires et sur la responsabilisation individuelle.

À cet égard, les membres de la communauté du Cégep doivent être sensibilisés :

- à la sécurité de l'information et des systèmes d'information du Cégep;
- aux conséquences d'une atteinte à la sécurité ;
- à leurs rôles et à leurs responsabilités en la matière.

Le Cégep s'engage, sur une base régulière, à sensibiliser et à former les utilisatrices et les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière. L'utilisatrice et l'utilisateur ont la responsabilité de participer à ces activités de sensibilisation et de formation.

ARTICLE 9 – SANCTIONS

En cas de contravention à la présente politique, l'utilisatrice ou l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information ne soit pas protégée adéquatement.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles administratives ou disciplinaires internes applicables.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au Cégep ou en vertu des dispositions de la législation applicable en la matière.

ADOPTION ET ENTRÉE EN VIGUEUR

La présente politique annule et remplace toute politique antérieure sur le même sujet. Elle a été adoptée par la résolution CA/2024-539-8.2 le 18 juin 2024 et est en vigueur depuis cette date.