Politique de sécurité de l'information

Date d'entrée en vigueur : 27/05/2025

Numéro de la résolution : 73-CA-2024-2025

Numéro de la politique : P-2025-STI-1

Service responsable : STI

Date de révision prévue : 27/05/2030

Centre
de services scolaire
Marie-Victorin
Québec

Nom	Objet	Version	Date
Josiane Paquette	Début de la rédaction	0.8	2023-03
Valentin Lalain - Ludovic Cambron	Prise en compte gabarit FCSSQ	0.8	2024-07-16
Gilles Lochet	Validation CSIO	0.9	2024-08-28
Secrétariat général	Validation et modifications mineures	0.9.1	2024-09-16
Comité consultatif de gestion	Recommandation	0.9.2	2024-12-04
Comité SI	Validation et modifications mineures	0.9.3	2024-12-12
Comité de vérification	Validation	0.9.5	2025.05.06
Conseil d'administration	Adoption	1.0	2025.05.27

TABLE DES MATIÈRES

CONTEXTE

Le Centre de services scolaires Marie-Victorin (CSS Marie-Victorin) reconnaît que l'information et les technologies qui la supportent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission. De plus, l'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c.G-1.03) (LGGRI) et la Directive gouvernementale sur la sécurité de l'information (décret 1514-2021) applicable aux organismes publics visés à l'article 2 de la LGGRI créent des obligations aux organismes scolaires en matière de sécurité de l'information.

Pour se conformer à ses obligations réglementaires et légales ainsi que pour atteindre des standards de sécurité de l'information élevés, le CSS Marie-Victorin a l'obligation d'adopter, de garder à jour et de veiller à l'application d'une politique de sécurité de l'information. Cette politique a pour objectif d'encadrer la gestion des risques, la gestion des accès aux actifs informationnels, la gestion des incidents, la gestion de la continuité des activités ainsi que tout processus disposant d'un lien avec la sécurité de l'information.

OBJECTIFS

La présente politique constitue le cadre général de gestion des actifs informationnels. Dans le respect des droits et obligations du CSS Marie-Victorin, elle vise à garantir l'atteinte des objectifs de sécurité de l'information et plus spécifiquement à :

- Assurer la protection de l'actif informationnel tout au long de son cycle de vie ;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon, sans autorisation préalable du responsable de l'actif ;
- Assurer la disponibilité de l'information pour qu'elle soit accessible au moment voulu et utilisable à la demande par les personnes et les outils technologiques autorisés;
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou de la divulguer à des personnes, entités ou processus non autorisés;
- Assurer la traçabilité des changements d'état de l'information;
- Regrouper les lignes directrices, les rôles et responsabilités des intervenants en sécurité de l'information;
- Identifier et catégoriser les actifs informationnels du CSS Marie-Victorin selon leur degré de criticité et assurer une vigie constante à leur évaluation ainsi que leur protection adéquate;
- Assurer la conformité aux lois et aux encadrements réglementaires.

Cadre légal et administratif

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 (L.R.Q. c. I-13.3);
- Le Code civil du Québec (LQ, 1991, chapitre 64);
- Le Code criminel (LRC, 1985, chapitre C-46);
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c.G-1.03);
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics.
- La Loi concernant le cadre juridique des technologies de l'information (RLRQ, C-1.1);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, 2.1);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- La Directive gouvernementale sur la sécurité de l'information (décret 1514-2021);
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- La Loi sur les archives (RLRQ, c.A-21.1);
- Le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (RLRQ, c. A-21.1, r.2);
- La Politique d'utilisation des ressources informatiques et des services de réseautique et de télécommunications (2009);
- La Politique relative à la gestion documentaire (AD-02-04, 2014).

CHAMP D'APPLICATION DE LA POLITIQUE

Personnes visées

La politique s'adresse aux utilisateurs de l'information ou des actifs informationnels du CSS Marie-Victorin. Elle s'applique à toute personne qui est au service, qui utilise ou qui est membres des instances et des comités du CSS Marie-Victorin, qu'elle travaille dans ses locaux ou à distance. Elle s'applique également à toute personne liée par contrat, par entente ou par prêt de service ainsi qu'à toute personne employée par un fournisseur du CSS Marie-Victorin dans l'accomplissement de son mandat.

Actifs visés

L'information visée est celle que le CSS Marie-Victorin, ou un tiers pour son compte, détient ou utilise dans l'exercice de ses fonctions, et ce, quel que soit le support de conservation, de traitement ou de transmission.

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 CSS Marie-Victorin, en tout lieu, en tout temps et sur tout support.

Cessation d'application

La présente politique cesse de s'appliquer au moment où l'information visée est détruite de façon complète et irréversible par le CSS Marie-Victorin.

RÔLES ET RESPONSABILITÉS

Direction générale

La direction générale fait adopter par le comité de la direction générale, les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de sécurité de l'information. Elle assume aussi le processus de délégation des rôles de chef de la sécurité de l'information organisationnelle (CSIO), de coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) et de responsable de la protection des renseignements personnels (RPRP).

Responsable de la protection des renseignements personnels (RPRP)

Le RPRP veille à assurer le respect et la mise en œuvre de la loi en regard à la protection des renseignements personnels. Le responsable met en œuvre des politiques et des pratiques encadrant la gouvernance des renseignements personnels.

Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation (article 10, premier alinéa, de la Directive gouvernementale sur la sécurité de l'information et l'article 22 du Cadre gouvernemental de gestion de la sécurité de l'information (CGGSI)). Il apporte à son dirigeant d'organisme le soutien nécessaire lui permettant d'assumer ses obligations en sécurité de l'information.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI agit sur le plan opérationnel. Il intervient dans la mise en œuvre des mesures et il soutient le CSIO du CSS Marie-Victorin, notamment en matière de la gestion des incidents et des risques en sécurité de l'information.

Le COMSI représente le CSS Marie-Victorin auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des

menaces, vulnérabilités et incidents (GMVI) du CSS Marie-Victorin, en soutien au CSIO.

Direction des technologies de l'information

La direction veille à l'intégration des exigences de sécurité dans l'utilisation quotidienne des systèmes et dans les nouveaux projets. En collaboration avec le CSIO, elle identifie des mesures de protection pour sécuriser les actifs informationnels en fonction de leur sensibilité, tout en respectant les exigences réglementaires et contractuelles

Direction des ressources humaines (DRH)

La DRH collabore avec le CSIO afin de :

- Sensibiliser les membres du personnel en matière de sécurité de l'information;
- Concevoir des contenus de sensibilisation destinés aux membres du personnel;
- Mettre en place et maintenir une gestion des identités et des accès adéquats.

Responsable d'actifs informationnels (détenteur)

Le responsable d'actifs informationnels est l'employé dont l'un des rôles consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous sa responsabilité. À ce titre, il :

- Participe à la classification de l'information 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 sécurité de l'information;
- Au besoin, collabore à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un incident.

Utilisateurs

La responsabilité de la sécurité de l'information du CSS Marie-Victorin incombe à tous les utilisateurs d'actifs informationnels. L'utilisateur qui accède à une information, qui la consulte ou qui la traite en est responsable et il doit donc contribuer à sa protection.
À cette fin, l'utilisateur doit :

- Se conformer à la présente politique et à toute autre directive et procédure du CSS Marie-Victorin 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 mot de passe et de son code d'accès, 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, ou son supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel;

- Au besoin, participer à la classification 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 ou un incident à la sécurité de l'information

PRINCIPES DIRECTEURS

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. L'organisation fonctionnelle concerne les rôles et responsabilités 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 menaces et des risques.
La politique de sécurité de l'information du CSS Marie-Victorin se base sur sept axes fondamentaux de gestion :

Gestion des identités et des accès (GIA)
La gestion des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le CSS Marie-Victorin soient strictement réservés aux personnes autorisées.

Gestion des vulnérabilités et des menaces
La gestion des vulnérabilités et des menaces se caractérise par la mise en application de mesures préventives ou correctives pour assurer la sécurité de l'information. Les mesures déployées visent à assurer la continuité des services. Dans la gestion des vulnérabilités et menaces, le CSS Marie-Victorin peut exercer ses pouvoirs et ses prérogatives en cas d'utilisation inappropriée de l'actif informationnel.

Gestion des risques
La gestion des risques concernant l'actif informationnel du CSS Marie-Victorin est basée sur une analyse des menaces encourues quant à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le CSS Marie-Victorin. De cette analyse découlent des mesures compensatoires relatives à l'utilisation et à l'opération des systèmes d'information ainsi qu'aux résultats escomptés.

Gestion des incidents
La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relatives aux incidents de sécurité et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services et minimiser les préjudices. Dans la gestion des incidents, le

CSS Marie-Victorin peut exercer ses pouvoirs et ses prérogatives en cas d'utilisation inappropriée de l'actif informationnel.

Gestion de la continuité des affaires, des services essentiels et de la reprise informatique

La gestion de la continuité des affaires, des services essentiels et de la reprise informatique se caractérise par la mise en place de processus et de procédures permettant de limiter les perturbations qui peuvent toucher et compromettre les opérations courantes les plus critiques. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités du CSS Marie-Victorin et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité et la reprise des activités critiques.

Respecter la propriété intellectuelle

Le CSS Marie-Victorin ainsi que tout son personnel se conforment aux exigences légales concernant l'utilisation des logiciels propriétaires et des logiciels libres, de même que des produits, des documents et de l'information qui pourraient être protégés par des droits de propriété intellectuelle.

Gestion de l'approvisionnement de solutions informatiques

Les ententes contractuelles sont gérées de manière diligente et comportent notamment des clauses visant le respect des exigences ministérielles en matière de sécurité de l'information.

Avant le début de tout mandat, tout fournisseur doit s'engager à respecter un engagement de confidentialité.

Les exigences en matière de SI sont prises en considération dès le début des études menant à l'acquisition ou au développement d'un système d'information. Les mesures de protection requises doivent être appliquées tout au long du processus de conception du système, lors de son exploitation et même, le cas échéant, à la fin de sa vie utile, lors de sa destruction.

Les exigences en matière de SI sont prises en considération lors du développement de système d'information. Les unités d'affaires détentrices du système d'information, ou en voie d'en acquérir un, les déclarent, s'assurent qu'ils sont catégorisés et gèrent les risques en matière de SI qu'ils comportent.

FORMATION, SENSIBILISATION ET INFORMATION

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

À cet égard, les utilisateurs des actifs informationnels du CSS Marie-Victorin doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du CSS Marie-Victorin;
- Aux conséquences d'une atteinte à la sécurité des actifs informationnels;
- À leur rôle et à leurs responsabilités en la matière.

Le CSS Marie-Victorin s'engage – sur une base régulière – à informer, à sensibiliser et à former 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 à leurs obligations à cet égard.

L'utilisateur a la responsabilité de participer à ces activités de sensibilisation et de formation.

SÉCURITÉ EN LIEN AVEC L'INTELLIGENCE ARTIFICIELLE

Le CSS Marie-Victorin établit les mesures de sécurité applicables aux services, logiciels et technologies utilisant l'intelligence artificielle. Ces mesures émanent, entre autres, du ministère de la Cybersécurité et du Numérique et des obligations liées à la protection des renseignements personnels. Le CSS Marie-Victorin s'assure de se conformer aux normes, obligations et lois en lien avec le développement et l'utilisation responsable de l'intelligence artificielle.

RÉVISION DE LA POLITIQUE

La politique doit être révisée annuellement à l'occasion de changements mineurs qui pourraient l'affecter. Elle est mise à jour entièrement au besoin tous les quatre ans (4) ans. La mise à jour est suggérée par le CSIO, le COMSI ou le comité en sécurité de l'information du CSS Marie-Victorin.

SANCTION

En cas de contravention à la présente politique, 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.

Quiconque 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 CSS Marie-Victorin ou en vertu des dispositions de la législation applicable en la matière.

DROIT DE REGARD

Le CSS Marie-Victorin exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels, et ce, dans le respect de la vie privée des utilisateurs.

ENTRÉE EN VIGUEUR

La présente politique est entrée en vigueur à la date de son adoption présente à la page 2 du document.

GLOSSAIRE

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 CSS Marie-Victorin pour mener à bien sa mission.

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 d'un sinistre majeur.

Risques liés à la sécurité de l'information : tout événement lors du traitement, de l'utilisation ou de l'entreposage comportant un degré d'incertitude, qui pourrait porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information et causer un préjudice.

Technologies de l'information : regroupent les techniques, 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.

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 CSS Marie-Victorin.

Information : un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Confidentialité : la propriété d'une information d'être accessible uniquement aux personnes ou entités désignées et autorisées et d'être divulguée qu'à celles-ci.

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

Intégrité : la propriété d'une information de ne subir aucune altération ni destruction sans autorisation ou de façon erronée, et qui est conservée sur un support et préservée avec des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.