Centre de services scolaire de la Vallée-des-Tisserands
Québec

# POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION, À L'UTILISATION DES RESSOURCES INFORMATIONNELLES ET À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

| | |
|---|---|
| Origine : Comité sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels<br>Résolution : CA-3894-250923<br>Date d'entrée en vigueur : 23 septembre 2025 | Mise à jour : |

## TABLE DES MATIÈRES

## 1. PRÉAMBULE

En vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et de la Directive sur la sécurité de l'information gouvernementale, le Centre de services scolaire de la Vallée-des-Tisserands (ci-après CSSVT) a des obligations en matière de sécurité de l'information, dont celle d'adopter une politique de sécurité de l'information, de la maintenir à jour et d'en assurer l'application, appuyée par un cadre de gestion. Le CSSVT a également la responsabilité d'assurer la protection des renseignements personnels qu'il détient aux termes de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

En raison de la nature sensible et confidentielle de l'information traitée par le CSSVT, la sécurité de l'information, l'utilisation des ressources informationnelles et la protection des renseignements personnels revêtent une importance capitale et doivent faire l'objet d'un ensemble intégré de mesures qui s'articulent à l'intérieur d'une structure de gouvernance bien définie. Le CSSVT est une institution protégée, résiliente et proactive en matière de sécurité de l'information et de protection des renseignements personnels et qui offre des services numériques aux membres de sa communauté.

L'adoption de la Politique permettra au CSSVT de réaliser sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information et les renseignements personnels dont il est le gardien.

L'émergence et l'accroissement rapide des technologies de l'information dans la société en général et dans le milieu de l'éducation en particulier ont entrainé l'introduction graduelle de nombreux équipements et technologies au CSSVT et l'expansion rapide de l'infrastructure du réseau, incluant les technologies gérées depuis l'infonuagique.

## 2. OBJECTIFS

La présente Politique a pour objectif d'affirmer l'engagement du CSSVT à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, de la protection des renseignements personnels et de l'utilisation des ressources informationnelles, quels que soient leurs supports ou leurs moyens de communication.

La Politique définit les principes, rôles et responsabilités pour protéger ses actifs informationnels, ainsi que pour assurer la protection des renseignements personnels. Elle indique les attentes du CSSVT liées à la sécurité de l'information, à la protection des renseignements personnels et à l'utilisation des ressources informationnelles.

Cette politique respecte les normes et la législation applicable en matière de sécurité de l'information et de protection des renseignements personnels.

Le CSSVT met en place la présente Politique dans le but d'orienter et de déterminer sa vision, appuyée par le Cadre de gouvernance sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels (ci-après nommé le « Cadre de gouvernance »).

## 3. CADRE LÉGAL

La Politique s'inscrit principalement dans un contexte régi par :

- Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- Code civil du Québec (LRQ, 1991, chapitre 64);
- Loi sur l'accès aux documents des organismes publics et protection des renseignements personnels (LRQ, chapitre A-2.1, R.2);
- Loi sur les archives (LRQ, A-21.1);
- Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);
- Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- Loi sur l'instruction publique (LRQ. C.L-13.3);
- Règlement du calendrier de conservation, versement, dépôt et élimination des archives publiques (LRQ. C-A-21.1, R.1);
- Politique gouvernementale de cybersécurité;
- Directive sur la sécurité de l'information gouvernementale;
- Cadre gouvernemental de gestion de la sécurité de l'information;
- Règlement sur les normes d'éthique et de déontologie applicables aux membres du conseil d'administration d'un centre de services scolaire francophone;
- Code d'éthique applicable aux membres du personnel et à toute personne appelée à œuvrer auprès d'élèves mineurs ou handicapés ou à être en contact avec eux du CSSVT.

## 4. DÉFINITIONS

| Terme | Définition |
|---|---|
| **Actif informationnel** | L'actif informationnel est un élément qui représente une valeur pour l'organisme. Il désigne toute donnée, information, système, infrastructure technologique ou ressource liée à l'acquisition, au traitement, à l'entreposage ou à la diffusion de l'information, qui est sous la responsabilité d'un organisme public. Cela inclut tant les contenus numériques que les supports physiques, dans le cadre de leurs gestion et protection. |
| **Confidentialité** | Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées. |
| **Continuité des services** | Capacité d'une organisation à maintenir ou à restaurer la poursuite de sa mission et de ses processus d'affaires à un niveau de service prédéfini, même en cas de sinistre ou d'incident majeur, en mettant en place des stratégies et des mesures adaptées. |
| **Cycle de vie des actifs informationnels** | Ensemble des étapes que franchisent les actifs informationnels, de leur création, leur enregistrement, leur transfert, leur consultation, leur traitement et leur transmission, jusqu'à leur conservation permanente ou leur destruction, en conformité avec le calendrier de conservation du CSSVT. |
| **Cycle de vie des renseignements personnels** | Le cycle de vie des renseignements personnels correspond à l'ensemble des étapes de traitement de ces renseignements personnels à partir de leur collecte, en passant par leur utilisation, leur communication à des tiers, leur conservation et leur destruction ou leur anonymisation. |
| **Disponibilité** | Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée. |
| **Document** | Un document est 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 ces formes ou en un autre système de symboles. |
| **Équipement technologique** | Ensemble des ressources matérielles de nature technologique utilisées pour le traitement, le stockage, la transmission ou l'affichage de données. Cela inclut notamment les ordinateurs de |

| Terme | Définition |
|---|---|
| | bureau, les ordinateurs portables, les écrans, les tablettes, les téléphones et appareils mobiles, les imprimantes, ainsi que les composantes du réseau informatique (routeurs, commutateurs, serveurs, etc.). |
| **Incident de confidentialité** | On entend par « incident de confidentialité » : (1) l'accès non autorisé par la loi à un renseignement personnel; (2) l'utilisation non autorisée par la loi d'un renseignement personnel; (3) la communication non autorisée par la loi d'un renseignement personnel; (4) la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement. |
| **Information** | Renseignement consigné sur un support quelconque (papier ou électronique) ou communiqué dans un but de transmission des connaissances. À titre d'exemple, l'information comprend les fichiers structurés (bases de données) et non structurés (fichiers Word, Excel, PowerPoint, PDF, etc.), les courriels, les messages texte, les communications et les messages vocaux, photos, dessins, télécopies, originaux et copies de documents papier, rapports informatisés ainsi que les copies de sauvegarde et les archives. |
| **Événement de sécurité** | Toute forme d'atteinte, présente ou appréhendée, telles une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité du CSSVT. |
| **Intégrité** | Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et être conservée sur support procurant stabilité et pérennité. |
| **Logiciel** | Ensemble d'instructions ou de données exprimées sous une forme lisible par une machine et destiné à exécuter une fonction ou à produire un résultat spécifique lorsqu'il est utilisé sur un ordinateur. Cette définition inclut les programmes, les systèmes d'exploitation, les applications bureautiques, ainsi que leurs composantes ou modules associés. |
| **Mesure de sécurité de l'information** | Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou réduire les pertes qui en résultent. |
| **Norme** | Accord entériné par un organisme officiel de normalisation, comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), 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. |
| **Pratique** | Savoir ou manière de faire qui conduisent au résultat souhaité et qui est porté en exemple afin de faire partager l'expérience qui permet une amélioration collective. |
| **Procédure** | Une procédure est une série de tâches reliées entre elles et formant une séquence préalablement définie qu'il faut accomplir pour produire un résultat. Elle précise le quoi, le comment, le quand et les intervenants. Les procédures sont des plans qui définissent les méthodes qui devront être utilisées dans l'exécution des activités prévues. Elles guident davantage l'action que la réflexion et expliquent en détail et de façon précise, la manière d'accomplir une certaine activité. Essentiellement, elles se distinguent par la séquence chronologique de leur contenu. La procédure doit être précise et ne laisser aucune place à l'interprétation. |
| **Processus** | Ensemble d'activités ou de tâches logiquement interreliées, organisées dans le but d'atteindre un objectif ou de produire un résultat spécifique, souvent en transformant des intrants en extrants. |
| **Renseignement personnel** | Renseignement concernant une personne physique et qui permet, directement ou indirectement, de l'identifier. Un renseignement personnel ayant un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel. |
| **Ressource informationnelle** | Ensemble des actifs informationnels et des ressources humaines, matérielles et financières directement impliqués dans la gestion, l'acquisition, le développement, l'entretien, l'exploitation, l'accès, l'utilisation, la protection, la conservation et l'aliénation de ces actifs. |
| **Sécurité de l'information** | Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. Elle englobe également d'autres propriétés essentielles telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, selon les besoins spécifiques. |
| **Standard** | Norme non définie ni entérinée par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), mais qui s'est imposée par la force des choses parce qu'elle fait consensus auprès des utilisateurs. |
| **Système d'information** | Ensemble organisé d'actifs informationnels, de ressources humaines, de processus et d'actifs physiques ou technologiques, interconnectés pour collecter, traiter, stocker, diffuser et gérer |

| Terme | Définition |
|---|---|
| | l'information, dans le but de soutenir un ou plusieurs objectifs d'affaires. |
| **Utilisateur** | Toute personne physique ou morale (membre du personnel, élève, parent, administrateur, représentant de la communauté, partenaire ou consultant) pour qui un code d'identification et un mot de passe ont été émis pour l'accès aux ressources informationnelles du CSSVT. |

## 5. CHAMPS D'APPLICATION

### 5.1. Priorité d'application

En cas d'incompatibilité ou de contradictions entre les dispositions de la présente Politique et celles de la *Politique sur l'utilisation des ressources informatiques et des médias sociaux* ou du *Code d'éthique en lien avec l'utilisation des ressources informatiques et des médias sociaux*, les dispositions de la présente Politique prévaudront. De plus, dans l'éventualité où un même sujet est abordé à la fois par la présente Politique et par la *Politique sur l'utilisation des ressources informatiques et des médias sociaux* ou par le *Code d'éthique en lien avec l'utilisation des ressources informatiques et des médias sociaux*, les dispositions de la présente Politique s'appliquent de manière prioritaire.

### 5.2. Personnes visées

La présente Politique s'adresse à tous les membres du personnel, peu importe le statut, ainsi qu'à toute personne physique ou morale qui, à titre d'élève, parent, administrateur, représentant de la communauté, partenaire, consultant, fournisseur ou visiteur a accès à des renseignements personnels ou conçoit, développe ou utilise des actifs informationnels du CSSVT ou y a accès.

### 5.3. Information visée

Tout actif informationnel et tout renseignement personnel que le CSSVT détient dans l'exercice de sa mission, que sa conservation soit assurée par elle-même ou par un tiers. La présente Politique porte sur les actifs informationnels et sur les renseignements personnels détenus ou utilisés par le CSSVT, peu importe leur nature, leur localisation ou leur support, et ce, durant tout leur cycle de vie. Elle couvre les domaines organisationnels, technologiques, physiques, environnementaux, la gestion documentaire et la gestion contractuelle.

### 5.4. Activités visées

Cette Politique concerne l'ensemble des activités entrant dans le cycle de vie des actifs informationnels et des renseignements personnels à savoir : la collecte, l'enregistrement, le traitement, la modification, la communication, la diffusion, la conservation et la destruction des actifs informationnels du CSSVT et des renseignements personnels, en tout lieu, en tout temps et sur tout support.

## 6. CONTENU

### 6.1. Principes directeurs

La sécurité de l'information et la protection des renseignements personnels visent à renforcer la confiance envers l'État et ses services, tout en soutenant sa mission par la pérennité d'une information fiable. Une démarche éthique favorisant la responsabilisation collective et individuelle encadre sa gestion. Les pratiques adoptées doivent être exemplaires, alignées sur les meilleures pratiques reconnues, et appliquées à l'échelle de l'organisation.

La sécurité de l'information et la protection des renseignements personnels relèvent d'une responsabilité collective. Chacun doit être formé, sensibilisé et rendre des comptes selon son rôle, avec une attribution claire des responsabilités et des processus de reddition efficaces.

### 6.2. Sécurité de l'information

Le CSSVT s'aligne sur les orientations stratégiques gouvernementales en matière de sécurité de l'information en adoptant des pratiques reconnues pour assurer la protection adéquate de ses actifs informationnels. Ces actifs, essentiels à la mission de l'organisation, font l'objet d'évaluations constantes et d'une protection adaptée à leur importance, leur confidentialité et leur exposition aux risques, d'erreur ou de malveillance. Une démarche éthique guide la sécurisation des actifs informationnels et la responsabilisation individuelle.

Le CSSVT prend également les mesures appropriées en cas d'événement de sécurité. Le CSSVT assure la sécurité des ressources informationnelles et de l'information qu'il détient ou utilise conformément aux principes fondamentaux énoncés dans la politique gouvernementale en matière de sécurité de l'information en vigueur, incluant toute modification à celle-ci, et aux cinq principes directeurs suivants :

*6.2.1. Éthique*

Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

*6.2.2. Évolution*

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement et actualisées afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des risques de sécurité de l'information afférents.

*6.2.3. Responsabilité et imputabilité*

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation et la mise en place de processus de gestion de la sécurité de l'information permettant une reddition de comptes adéquate.

*6.2.4. Transparence*

L'information concernant les événements de sécurité, les pratiques et les solutions de sécurité de l'information afférentes doit être communiquée avec fluidité au sein de l'Administration publique, sous réserve du droit applicable.

*6.2.5. Universalité*

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

### 6.3. Protection des renseignements personnels

Le CSSVT est responsable de la protection des renseignements personnels qu'il détient tout au long de leur cycle de vie. À cet effet, il prend les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Le CSSVT prend également les mesures appropriées en cas d'incident de confidentialité.

### 6.4. Confidentialité

Les communications via les actifs informationnels ne sont pas totalement confidentielles ni entièrement sécurisées. Les mots de passe et codes d'accès protègent les informations du CSSVT contre les tiers, sans garantir la confidentialité des messages du personnel.

Pour assurer au CSSVT un accès continu à ses systèmes, les utilisateurs ne doivent pas utiliser de logiciels personnels ou non approuvés pour chiffrer leurs courriels, boîtes vocales ou autres informations, sauf avec l'autorisation préalable de leur supérieur et l'approbation du Chef de la sécurité de l'information organisationnelle (CSIO).

L'information contenue dans les actifs informationnels du CSSVT est confidentielle si elle inclut des renseignements personnels ou tout renseignement protégé en vertu de lois, règlements, contrats ou ententes de confidentialité.

### 6.5. Respect de la propriété intellectuelle

L'organisation du CSSVT 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.

### 6.6. Utilisation des ressources informationnelles

- L'utilisation des ressources informationnelles du CSSVT est un privilège qui peut être suspendu ou révoqué en cas de non-respect de la présente Politique ou de tout autre écrit de gestion découlant du Cadre de gouvernance. Ces ressources doivent être utilisées en priorité pour soutenir les activités liées à la mission du CSSVT;

- Tout accès ou tentative d'accès non autorisé aux actifs informationnels est interdit;
- Les utilisateurs doivent respecter les conditions d'utilisation des logiciels, applications, sites et services en ligne, y compris les médias sociaux. Toute utilisation à des fins commerciales, illicites, frauduleuses, diffamatoires, discriminatoires ou incitant à la haine, à la violence, au racisme ou au sectarisme est strictement interdite;
- L'utilisateur doit respecter les mesures de sécurité des actifs contenant des données sensibles, en utilisant des mots de passe complexes et sans altérer les configurations de sécurité;
- Les utilisateurs doivent s'abstenir de toute action perturbant les équipements, notamment l'insertion ou la propagation de virus;
- Les actifs contenant des données confidentielles doivent être protégés par un mécanisme d'identification et d'authentification. L'accès est réservé aux personnes autorisées selon la nature des informations et des applications;
- L'utilisateur est responsable de la confidentialité de ses codes d'accès et doit garantir leur protection contre tout accès non autorisé. Il est strictement interdit à l'utilisateur de tenter de décrypter ou de découvrir les codes d'accès d'un autre utilisateur;
- L'utilisateur doit s'identifier avec son propre code d'accès et ne pas usurper l'identité d'autrui. Toute exception requiert l'autorisation du DSRI;
- Au départ du CSSVT, restituer tous les actifs informationnels, équipements informatiques ou téléphoniques attribués;
- Les utilisateurs doivent signaler sans délai à la direction de l'unité administrative toute violation ou anomalie compromettant la protection des actifs informationnels du CSSVT.

### 6.7. Surveillance des actifs informationnels

Le CSSVT peut exercer tout mécanisme de surveillance, notamment accéder, récupérer, lire et divulguer, les communications (notamment les courriels, conversations et tout autre type de communications) et informations qui résident et transigent sur ses actifs informationnels lorsque des motifs raisonnables et légitimes le justifient.

Il peut également intervenir s'il a des raisons de croire qu'un utilisateur adopte ou s'apprête à adopter un comportement inapproprié en lien avec ses actifs informationnels.

### 6.8. Cadre de gouvernance

Cette Politique est soutenue par le Cadre de gouvernance, qui définit les directives, processus, procédures et meilleures pratiques nécessaires à sa mise en œuvre en se basant sur les normes et standards de l'industrie. Ce cadre assure la cohérence et l'harmonisation des actions entreprises au sein de l'organisation pour garantir la conformité et la sécurité, tout en favorisant l'amélioration continue des pratiques de gestion des informations et renseignements personnels.

## 7. RÔLES ET RESPONSABILITÉS

### 7.1. Conseil d'administration

- Adopte la présente Politique;
- Nomme le chef de la sécurité de l'information organisationnelle (CSIO), sur recommandation de la direction générale;
- Nomme les coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI), sur recommandation de la direction générale.

### 7.2. Direction générale

- Recommande l'adoption de la Politique au conseil d'administration;
- Assure l'application de la Politique;
- Recommande la nomination du CSIO, du ou des COMSI au conseil d'administration;
- Veille à assurer le respect et la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- Désigne le responsable de la protection des renseignements personnels, mets en place des mesures pour préserver son autonomie et veille à faciliter l'exercice de ses fonctions;
- Avise dès que possible la Commission d'accès à l'information par écrit du titre, des coordonnées et de la date d'entrée en fonction du responsable de la protection des renseignements personnels;
- Établit, par directive, les conditions et les modalités suivant lesquelles les renseignements peuvent être communiqués sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide, par les membres du personnel;
- S'assure de la mise en place et du bon fonctionnement du comité sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels et siège sur ce comité;
- Adopte le Cadre de gouvernance et les écrits de gestion qui en découlent. Elle voit également à leur mise à jour au besoin;
- Approuve les demandes de surveillance et la suspension des privilèges d'accès aux systèmes informatiques lorsque nécessaire;
- Se réserve le droit d'engager toute intervention appropriée pour surveiller les systèmes d'information et les actifs informationnels.

### 7.3. Comité sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels

- Approuve la Politique auprès de la direction générale;
- Approuve les modifications à apporter à la Politique pour l'adapter à de nouvelles circonstances, notamment lors d'un changement à la législation;
- Approuve le Cadre de gouvernance et les écrits de gestion qui en découlent auprès de la direction générale;
- Recommande la dérogation à un écrit de gestion relatif à la sécurité de l'information, sur demande ou recommandation soumises par le CSIO;

- Examine, priorise et recommande aux instances les orientations, les initiatives ainsi que les projets de sécurité de l'information et de protection des renseignements personnels;
- Approuve les plans d'action en matière de cybersécurité et de protection des renseignements personnels;
- Approuve la catégorisation des actifs informationnels proposée par les fiduciaires des données institutionnelles;
- Examine, priorise et recommande aux instances les plans d'action en lien avec le traitement d'événements de sécurité et d'incidents de confidentialité;
- Traite les événements de sécurité à portée organisationnelle et gouvernementale;
- Soutient le responsable de la protection des renseignements personnels dans l'exercice des responsabilités et dans l'exécution des obligations prévus à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- Soutient le Chef de la sécurité de l'information organisationnelle dans l'exercice des responsabilités et dans l'exécution des obligations prévues à *Loi sur la gouvernance et la gestion des ressources informationnelles;*
- Exerce toute autre fonction en lien avec la sécurité de l'information et la protection des renseignements personnels à la demande de la direction générale.

### 7.4. Responsable de la protection des renseignements personnels (PRRP)

- Veille à assurer le respect et la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
- Met en œuvre les règles encadrant la gouvernance des renseignements personnels du CSSVT;
- Gère les incidents de confidentialité et mets en place un registre des incidents de confidentialité;
- Exerce toute autre fonction en lien avec la protection des renseignements personnels à la demande de la direction générale.

### 7.5. Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO, membre du personnel d'encadrement du CSSVT, a pour rôle principal de mettre en œuvre les décisions prises par le chef gouvernemental de la sécurité de l'information (CGSI) et son chef délégué de la sécurité de l'information (CDSI).

- Met en œuvre les obligations et directives gouvernementales de sécurité de l'information;
- Mets en œuvre la gouvernance de la sécurité de l'information au sein de son organisation;
- Assure l'intégration des exigences de sécurité de l'information dans les projets ;
- Avise le CDSI en cas de risque majeur lié à un événement de sécurité;
- Gère les événements de sécurité et mets en place un registre des événements de sécurité;
- Représente l'organisation auprès du CGSJ et du CDSI;
- Coordonne le comité sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels et les sous-comités qui en découlent le cas échéant;

- Développe les compétences en sécurité de l'information du personnel de son organisation.

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

- Soutient le CSIO dans la mise en œuvre des mesures de sécurité et des recommandations des professionnels à la suite des audits de sécurité;
- Agit sur le plan opérationnel et interviens dans la mise en œuvre des mesures de sécurité;
- Représente l'organisation auprès du Réseau d'alerte gouvernemental;
- Applique le processus de gestion des menaces, vulnérabilités et incidents (GMVI) du CSSVT;
- Maintient le registre des événements de sécurité;
- Effectue et participe aux analyses de risques en sécurité de l'information;
- Gère le processus de gestion de déclaration des incidents et de résolution de problèmes et contribue à sa mise en place;
- Assure l'élaboration, la mise à jour et l'application d'un plan interne de réponse aux MVI
- Veille à la protection des actifs informationnels du CSSVT;
- Contribue au processus formel de gestion des droits d'accès à l'information;
- Planifie, définit, conçoit et intègre la sécurité de l'information dans tous les actifs informationnels pour maintenir et améliorer la performance et la conformité du CSSVT en matière de sécurité de l'information;
- Participe à la définition de la stratégie de cyberdéfense du CSSVT;
- Effectue les redditions de comptes requises aux différents paliers gouvernementaux en matière de sécurité de l'information et sur la mise en œuvre des plans de remédiation des risques;
- Gère les événements de sécurité;
- Membre obligatoire et contribue au Réseau de cyberdéfense du CSSVT;

### 7.7. Direction des Services des ressources informationnelles (DSRI)

- Met en place les mesures de protection, de détection, de prévention et de correction pour assurer la disponibilité, la confidentialité, et l'intégrité des actifs informationnels de même que la continuité des activités de l'organisation. Ces mesures préviennent les accidents, l'erreur, la malveillance, l'indiscrétion ou la destruction d'information sans autorisation;
- Veille à l'intégration des exigences de sécurité dans l'utilisation quotidienne des systèmes et dans les nouveaux projets;
- Collabore avec le CSIO, identifie les mesures de protection pour sécuriser les actifs informationnels en fonction de leur sensibilité;
- Agit en tant qu'administrateur du réseau informatique et peut suspendre les privilèges d'accès aux systèmes d'information ou tout autre actif informationnel;
- Autorise une surveillance des actifs informationnels conformément aux exigences et mesures de sécurité gouvernementales.

### 7.8. Direction des Services des ressources humaines (DSRH)

- Collabore au programme de sensibilisation des membres du personnel en matière de sécurité de l'information et de protection des renseignements personnels;
- Collabore à la conception des contenus de sensibilisation destinés aux membres du personnel;
- Collabore auprès du CSIO et des instances syndicales dans la mise en œuvre des mesures de sécurité qui impactent les membres du personnel;
- Collabore à l'élaboration des processus et procédures opérationnelles ayant trait à la sécurité de l'information à l'embauche, au départ ou au mouvement du personnel.

### 7.9. Direction des Services des ressources matérielles - Opérations (DSRMO)

- Assure la sécurité physique et la gestion des accès des bâtiments;
- Collabore avec la DSRI et le CSIO à la protection des actifs informationnels, notamment en ce qui a trait aux systèmes informationnels de gestion des actifs immobiliers et des locaux qui hébergent des actifs informationnels ou des données.

### 7.10. Responsable d'actifs informationnels (détenteur)

Le responsable d'actifs informationnels est le membre du personnel dont le rôle 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 catégorisation de l'information sous sa responsabilité et à l'analyse des risques ;
- Veille à la protection de l'information et des systèmes d'information en conformité avec la politique de sécurité de l'information ;
- Collabore à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un événement de sécurité et/ou à un incident de confidentialité.

### 7.11. Membres du personnel, élèves, parents, administrateurs, représentants de la communauté, partenaires, consultants, fournisseurs et visiteurs

- Prendre connaissance de la présente politique et des écrits de gestion liés et y adhérer;
- Utiliser et protéger les actifs informationnels mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place sur les équipements technologiques mis à leur disposition et contenant des données à protéger, sans modifier leur configuration ou les désactiver;
- Pour les personnes visées, respecter leurs obligations prévues au *Règlement sur les normes d'éthique et de déontologie applicables aux membres du conseil d'administration d'un centre de services scolaire francophone* ou au *Code d'éthique applicable aux membres du personnel et à toute personne appelée à œuvrer auprès d'élèves mineurs ou handicapés ou à être en contact avec eux* du CSSVT, selon le cas;

- Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;
- Signaler immédiatement à la direction de l'unité administrative tout acte dont il a connaissance et qui est susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CSSVT ou à la protection des renseignements personnels;
- Signaler tout événement de sécurité ou tout incident de confidentialité à la direction de l'unité administrative;
- Remettre les différentes cartes d'identité, d'accès, les actifs informationnels ainsi que tout l'équipement technologique mis à sa disposition par le CSSVT.

## 8. DROIT DE REGARD ET SANCTIONS

Le CSSVT exerce un droit de regard sur tout usage de ses actifs informationnels qui s'étend non seulement aux opérations effectuées à partir des équipements, mais également de tout autre équipement, personnel ou professionnel, susceptible de saisir, accéder, conserver ou de reproduire l'information du CSSVT.

Des vérifications périodiques peuvent être effectuées pour évaluer la performance des mesures de sécurité mises en œuvre pour assurer la protection de l'information de l'organisation et des renseignements personnels. Elles sont soutenues par un processus rigoureux et effectué par des personnes dûment habilitées et ciblent aussi toute activité contrevenant aux cadres légaux, réglementaires et administratifs, et ce, dans le respect de la vie privée des utilisateurs.

Toute personne qui enfreint une règle applicable à la sécurité de l'information ou à la protection des renseignements personnels est passible notamment de l'une des sanctions suivantes :

- La restriction de ses droits d'utilisation d'actifs informationnels visés par la présente Politique;
- Le remboursement au CSSVT de toute somme que ce dernier serait dans l'obligation d'encourir à la suite d'une utilisation non autorisée, frauduleuse ou illicite des actifs informationnels visés par la présente Politique;
- Dans le cas des membres du personnel, des mesures administratives ou des sanctions disciplinaires conformément aux conventions collectives ou aux règlements sur les conditions d'emploi des cadres ou hors cadres ainsi qu'aux lois en vigueur;
- Dans le cas des élèves, les sanctions sont prévues au code de vie de l'établissement fréquenté;
- Pour les partenaires mandataires ou les fournisseurs, les contrats en vigueur peuvent être résiliés et des dommages et intérêts pourraient leur être réclamés. De plus, les personnes qui travaillent pour ceux-ci peuvent se voir expulser des lieux de travail du CSSVT.

Le CSSVT peut transmettre à toute autorité judiciaire les renseignements colligés et qui la portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise. Des poursuites criminelles ou pénales pourraient être entreprises contre toute personne qui enfreindrait l'une de ces règles.

## 9. RESPONSABLES DE L'APPLICATION ET DE LA DIFFUSION

- La direction générale est responsable de l'application de la présente politique;
- Le secrétaire général assure la diffusion et la mise à jour de la présente politique.

Le personnel cadre doit soutenir le CSIO et le responsable de la protection des renseignements personnels dans l'exécution de ses obligations. Plus particulièrement, les Services des ressources humaines, des ressources informationnelles et les Services du secrétariat général et des communications peuvent développer des outils de formation et d'information applicables à l'embauche du personnel ou lors d'un mouvement.

## 10. ENTRÉE EN VIGUEUR

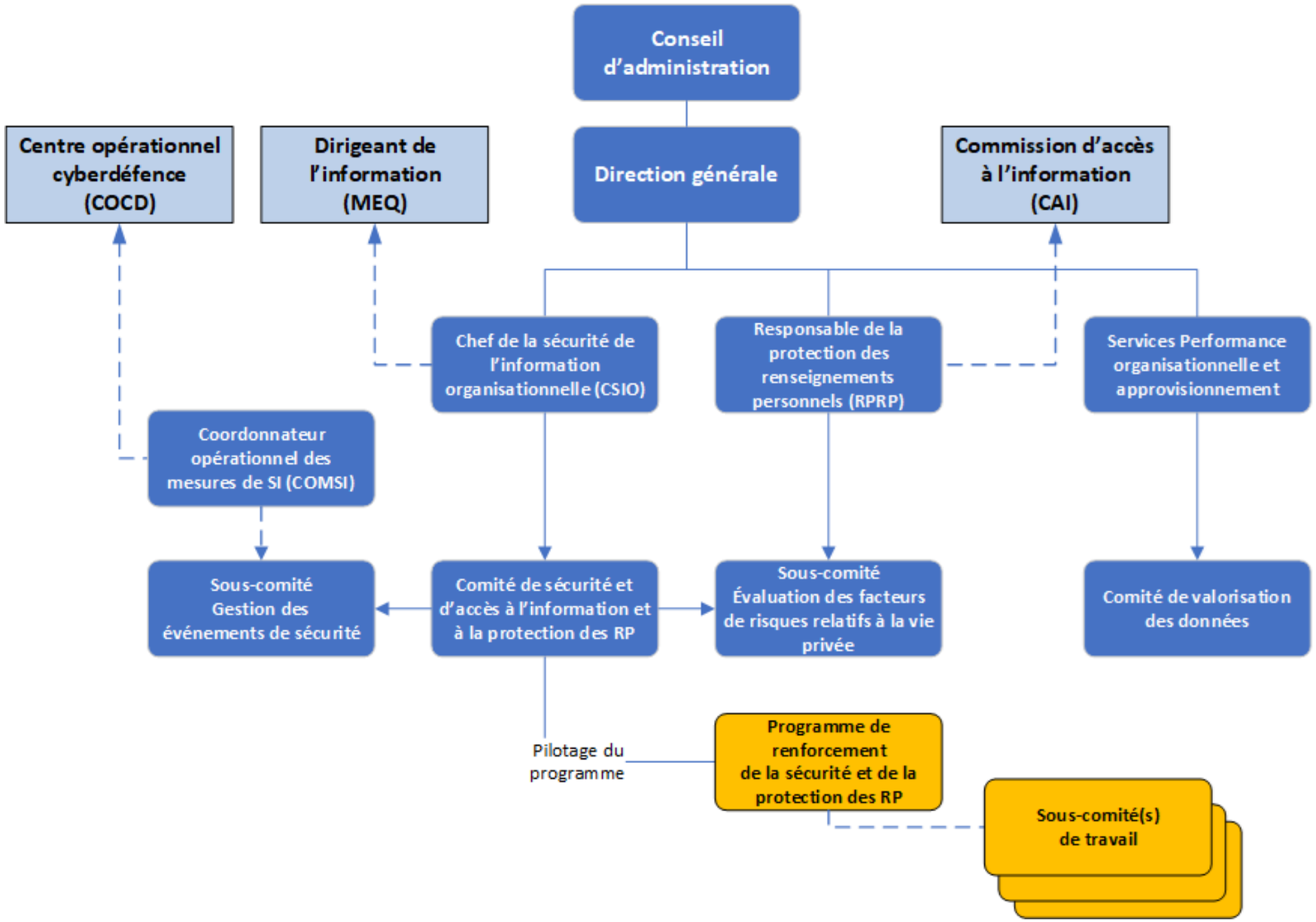
La présente politique est entrée en vigueur à la date de son adoption par le conseil d'administration.

Elle est révisée au minimum tous les trois ans à compter de sa date d'adoption, et ce, afin de tenir compte des changements juridiques, organisationnels, humains et technologiques ainsi que de l'évolution des menaces et des risques.

**ANNEXE I – STRUCTURE DE GOUVERNANCE**

Centre de services scolaire de la Vallée-des-Tisserands
Québec

## Structure de gouvernance de la sécurité et d'accès à l'information et à la protection des renseignements personnels



**ANNEXE II – RESSOURCES INFORMATIONNELLES**

**Définitions**

- Ressources informationnelles
- Actifs informationnels
- Réseau de télécommunication
- Système d'information
- Système informatique
- Équipements technologiques
- Internet, Intranet