POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

- Adoptée au conseil d'administration du 29 novembre 2017

Direction des ressources financières et de l'informatique

Table des matières

1. Préambule

La présente politique a pour but de permettre au Cégep de Sorel-Tracy d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information numérique et en support papier (actifs informationnels) qu'il a créée ou reçue (dont il est le gardien). Cette information est multiple et diversifiée. Elle implique des renseignements personnels d'étudiants et de membres du personnel, de l'information professionnelle sujette à des droits de propriétés intellectuelles (professeurs et chercheurs) et, finalement, de l'information stratégique ou opérationnelle pour l'administration du Cégep.

Le monde d'aujourd'hui n'a plus de frontières, il est ouvert à des pirates modernes en quête d'argent ou de prestige. Ces pirates, cachés dans un espace numérique parfois proche, parfois très éloigné, recherchent les faiblesses des systèmes en place pour réussir à accéder à notre information. Notre Cégep, faisant partie du réseau de l'enseignement supérieur, a une mission publique et est donc une cible potentielle.

Dans ce contexte, l'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre. G1.03) ainsi que la *Directive sur la sécurité de l'information gouvernementale* (une directive du Conseil du trésor du Québec applicable au Cégep) crée des obligations aux établissements collégiaux en leur qualité d'organismes publics. Ainsi, la *Directive sur la sécurité de l'information gouvernementale* prévoit que le Cégep adopte, met en œuvre, maintient à jour et assure l'application d'une politique de sécurité de l'information, dont les principales modalités sont définies dans la directive gouvernementale en ayant recours, notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des accès, la gestion des risques et la gestion des incidents.

DÉFINITIONS

Actifs informationnels : Tout système ou équipement permettant le traitement, le transport et l'entreposage de toute forme de communication ou d'information. Notamment, les équipements informatiques (poste de travail, ordinateur portatif, imprimante, etc.), les réseaux de communication (Internet, réseau local, réseau sans fil, réseau étendu, etc.), les systèmes de téléphonie et de télécommunication, le courrier électronique, les bases de données, les applications informatiques et les progiciels ainsi que la documentation nécessaire à leur bon fonctionnement. Inclus aussi toutes les informations inscrites sur support papier, électronique ou autres produites ou reçues dans le cadre des opérations.

Utilisateurs : tout le personnel, toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public, utilise les actifs informationnels du Cégep.

OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le Cégep doit veiller à:

- la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;

- l'intégrité de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

Par conséquent, le Cégep met en place cette politique dans le but d'orienter et de déterminer sa vision qui sera détaillée dans le cadre de gestion de la sécurité de l'information du Cégep.

Le cadre de gestion de la sécurité de l'information renforce les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du Cégep en matière de réduction du risque associé à la protection de l'information.

CADRE LÉGAL ET ADMINISTRATIF

La politique de sécurité de l'information s'inscrit principalement dans un contexte régi par :

- la *Charte des droits et libertés de la personne* (LRQ, chapitre C-12);
- le *Code civil du Québec* (LQ, 1991, chapitre 64);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;*
- 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 concernant le cadre juridique des technologies de l'inform*ation (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 sur les archives* (LRQ, chapitre A-21.1);
- le *Code criminel* (LRC, 1985, chapitre C-46);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 2);
- la *Directive sur la sécurité de l'information gouvernementale*;
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- la *Loi canadienne antipourriel* (LCAP, C-28);
- le *Code de vie étudiant du Cégep de Sorel-Tracy*;
- autres politiques et règlements du Cégep.

CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public, utilise les actifs informationnels du Cégep.

L'information visée est celle que le Cégep détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports, qu'ils soient numériques ou papiers, sont concernés.

2. Principes directeurs

Le Cégep s'appuie sur des principes directeurs en matière de sécurité de l'information qui le guide afin de :

- s'assurer de bien connaître l'information à protéger, en identifier les responsables et leurs caractéristiques de sécurité (principe qui confirme l'importance de maintenir à jour l'inventaire des actifs informationnels);
- s'appuyer sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires;
- adhérer à une approche basée sur le risque acceptable (la mise en place du cadre de gestion étant un moyen d'ajuster le risque, par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information, à un coût proportionnel à la sensibilité de l'information et aux effets potentiels);
- reconnaître l'importance de la politique de sécurité de l'information, du cadre de gestion de la sécurité de l'information qui doit être articulé par l'équipe informatique compétente et suffisante en nombre (cette équipe devant définir, mettre en place, opérer et ajuster la gestion de la sécurité de l'information);
- protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;
- mettre en place une gestion de la sécurité de l'information qui reconnaît que l'environnement technologique est en changement constant et interconnecté avec le monde et qui s'adapte à ces changements
- reconnaître l'importance d'évaluer régulièrement les risques, de mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, de définir des actions d'éradication des menaces ou de recouvrement des activités compromises;
- protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction (le niveau de sécurité pouvant varier au cours du cycle de vie du document);
- adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les organismes publics;
- sensibiliser à des principes éthiques visant à assurer le code de conduite et la responsabilisation individuelle (chaque individu qui a accès à l'information étant responsable de respecter les critères de disponibilité, d'intégrité et de confidentialité de celle-ci);
- s'assurer que chaque employé doit avoir accès à l'information requise pour accomplir ses tâches normales;
- communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels, afin que chacun puisse comprendre l'importance d'appliquer la sécurité comme on le demande, être informé de telle sorte qu'il puisse reconnaître les incidents de sécurité et agir en conséquence;
- mettre en place un plan de continuité des services en vue de rétablir les services essentiels aux utilisateurs, en cas d'interruption de services.

3. Cadre de gestion

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question 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 Cégep s'articule autour de trois axes fondamentaux de gestion. Ces axes sont la gestion des accès, la gestion des risques et la gestion des incidents.

GESTION DES ACCÈS

La gestion des accès doit être encadrée, mise en place et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le but de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des personnes, à tous les niveaux d'utilisateurs d'information du Cégep.

GESTION DES RISQUES

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse des risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Cégep. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance;
- des probabilités d'accident, d'erreur ou de malveillance auxquelles elle est exposée;
- des conséquences de la matérialisation de ces risques;
- du niveau de risque acceptable par le Cégep.

GESTION DES INCIDENTS

Le Cégep déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'obtention des buts suivants :

- limiter l'occurrence des incidents en matière de sécurité de l'information;
- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*. (par le CERT/AQ)

Selon la nature des incidents, la direction des ressources financières et informatiques du Cégep peut exercer ses pouvoirs et ses prérogatives, eut égard à toute utilisation inappropriée de l'information ou de ses systèmes d'information. Dans le cas d'un incident majeur, le comité d'enquête sera mis en place, tel que défini dans l'article 7.1 du *Règlement numéro 12* : *Règlement sur l'utilisation des technologies informatiques et internet*, ci-joint à l'annexe 1.

4. Rôles et responsabilités

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités de chacun des intervenants du Cégep par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate.

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'ils exercent.

CONSEIL D'ADMINISTRATION

Le conseil d'administration adopte la *Politique sur la sécurité de l'information* ainsi que toute modification à celle-ci. Le conseil d'administration est régulièrement informé des actions du Cégep en matière de sécurité de l'information. Il est le dirigeant de l'organisme responsable de l'application de la *Politique sur la sécurité de l'information* et il en délègue la responsabilité au directeur général.

COMITÉ DE DIRECTION

Le comité de direction du Cégep détermine des mesures visant à favoriser l'application de la politique et des obligations légales du Cégep en matière de sécurité de l'information. Ainsi, il détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information. Il peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

COMITÉ DE TRAVAIL POUR LA SÉCURITÉ DE L'INFORMATION

Le comité est formé du directeur des ressources financières et de l'informatique ainsi que du responsable de la sécurité de l'information. Le comité s'adjoindra des collaborateurs notamment sur les sujets suivants:

- informatique : ressources informatiques;
- support papier et archivage : secrétariat général;
- mobilier et bâtiment : ressources matérielles;
- confidentialité, employés : secrétariat général et ressources humaines;
- autres : au besoin.

Le comité de travail pour la sécurité de l'information a comme objectif d'assister le responsable de la sécurité de l'information à mettre en place le cadre de gestion de la sécurité de l'information et

autres éléments pouvant être nécessaires pour assurer la protection du Cégep et être conforme à la réglementation. Il consistera en un comité temporaire, planifié au besoin, qui traitera de sujets stratégiques, techniques et opérationnels.

Ce comité est chargé en particulier de mettre en place le cadre de gestion, les plans d'action et les bilans de sécurité de l'information, les activités de sensibilisation ou de formation ainsi que toutes propositions d'action en matière de sécurité de l'information. C'est aussi un forum d'échange entre les parties prenantes ou d'observation de l'évolution du projet en sécurité de l'information.

Ce comité collabore avec le service des ressources humaines et des communications du Cégep à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci.

DIRECTION GÉNÉRALE

La direction générale veille à l'application de la *Politique sur la sécurité de l'information*.

La direction générale :

- encadre le responsable de la sécurité de l'information dans la réalisation de son mandat;
- délègue certaines responsabilités au secrétaire général pour la gestion de l'information;
- fait adopter par le conseil d'administration 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;
- autorise, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du Cégep et d'en informer le conseil d'administration;
- autorise la création d'un comité d'enquête, si une enquête est requise. Cette autorisation au préalable peut provenir de la direction générale ou de la direction des ressources humaines et des communications et sa constitution devra respecter l'article 7.1 du *Règlement numéro 12* : *Règlement sur l'utilisation des technologies informatiques et internet*;
- met à jour le registre des dérogations et le registre des cas de contravention à la présente politique;
- fait le suivi auprès du comité de direction et du conseil d'administration.

RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

Le responsable de la sécurité de l'information est délégué et nommé par le conseil d'administration. Il relève du directeur général au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins.

Le responsable de la sécurité de l'information :

- élabore et propose le programme de sécurité de l'information du Cégep, rend compte de son implantation au comité de direction;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et met à jour la politique;
- assure la coordination et la cohérence des actions menées au sein du Cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels (directeurs et directeurs adjoints) du collège;
- produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;
- propose des recommandations et dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- s'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- collabore, si requis, aux enquêtes, comme personne-ressource, lorsqu'il y a ou pourrait y avoir transgression de la politique et si son expertise est susceptible d'aider le comité d'enquête dans la conduite de son investigation;
- assure des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

DIRECTION DES RESSOURCES FINANCIÈRES ET DE L'INFORMATIQUE

En matière de sécurité de l'information, la direction des ressources financières et de l'informatique s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient.

La direction des ressources financières et de l'informatique :

- participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information;
- applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que, par exemple, l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause ainsi que le cadre de gestion, soit la gestion des accès, des risques et des incidents.
- communique régulièrement de l'information au directeur général.

DIRECTION DES RESSOURCES MATÉRIELLES

La direction des ressources matérielles participe et collabore, avec le comité de travail pour la sécurité de l'information ou directement avec le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

DIRECTION DES RESSOURCES HUMAINES ET DES COMMUNICATIONS

En matière de sécurité de l'information, la direction des ressources humaines et des communications doit obtenir l'engagement au respect de la politique de tous les employés du Cégep.

Si une enquête est requise, la direction des ressources humaines et des communications pourra autoriser la création d'un comité d'enquête. Cette autorisation au préalable peut provenir de la direction générale ou de la direction des ressources humaines et des communications et sa constitution devra respecter l'article 7.1 du *Règlement numéro 12* : *Règlement sur l'utilisation des technologies informatiques et internet*.

RESPONSABLES D'ACTIFS INFORMATIONNELS (DIRECTEURS ET DIRECTEURS ADJOINTS)

Le rôle des responsables d'actifs informationnels (directeurs et directeurs adjoints) consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous leur responsabilité.

Les responsables d'actifs informationnels :

- informent tout utilisateur relevant de leur autorité de la politique de sécurité de l'information et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de se conformer aux règles;
- collaborent activement à la catégorisation de l'information sous leur responsabilité et à l'analyse de risques;
- voient au respect de la protection de l'information sous leur responsabilité et veille à ce que celle-ci soit utilisée par le personnel relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion;
- s'assurent que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous leur responsabilité et voient à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion;
- rapportent au directeur des ressources financières et de l'informatique toute menace ou tout incident afférent à la sécurité de l'information;
- collaborent à la mise en œuvre de toute mesure visant à améliorer ou à remédier à un incident ainsi qu'à toute opération de vérification de la sécurité de l'information;
- rapportent au directeur général ou au directeur des ressources humaines et des communications tout problème lié à l'application de la présente politique, dont toute dérogation / infraction réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

UTILISATEURS

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs des actifs informationnels du Cégep.

Tout utilisateur qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette information.

L'utilisateur doit :

- se conformer à la présente politique et à tout autre règlement et directive du Cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- 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 de ses fonctions et aux fins auxquelles ils sont destinés;
- participer au processus de catégorisation prévu qui permet d'évaluer le degré de sensibilité de l'information, dans le but de déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité (DIC) de l'information. Une prise d'inventaire de tout ce qui existe en information devra être établie et en fonction du degré de sensibilité déterminé, le Cégep pourra mettre en place les mesures permettant de se conformer aux obligations légales, d'éviter des pertes financières et d'atteindre les objectifs en ce qui a trait à la sécurité;
- respecter les mesures de sécurité mises en place, ne pas les contourner, ni modifier leur configuration, ni les désactiver;
- signaler à la direction tout incident susceptible de constituer une dérogation / infraction à la présente politique ou de constituer une menace à la sécurité de l'information du Cégep;
- 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.

Aussi, tout utilisateur des actifs informationnels du Cégep doit se conformer aux politiques, aux règlements et aux directives en vigueur avec lesquels il est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

5. Sensibilisation et information

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, tous les utilisateurs du Cégep doivent être sensibilisés :

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

À ces fins, des activités de sensibilisation et de formation seront offertes au moment opportun. De plus, des documents explicatifs seront disponibles sur le site Internet du Cégep.

6. Sanctions

En cas de dérogation / infraction à la présente politique, l'utilisateur s'engage personnellement; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

Tout utilisateur qui contrevient 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 dérogation / infraction en vertu du cadre légal et administratif.

De même, toute dérogation / infraction à la politique, qu'elle soit commise par le personnel, par toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public, utilisent les actifs informationnels du Cégep, est passible des sanctions prévues au contrat le liant au Cégep ou en vertu des dispositions de la législation applicable en la matière, tel le *Règlement numéro 12* : *Règlement sur l'utilisation des technologies informatiques et internet*.

Tout étudiant qui contrevient à une disposition du présent document est passible d'une sanction proportionnelle à la gravité de son acte et en tenant compte de récidive, s'il y a lieu. Les sanctions peuvent prendre la forme d'une réprimande, d'une expulsion immédiate, d'une suspension temporaire ou d'un renvoi.

7. Diffusion et mise à jour de la politique

Le comité de travail pour la sécurité de l'information et le responsable de la sécurité informatique sont responsables de la diffusion et de la mise à jour de la politique. La politique de sécurité de l'information sera révisée tous les cinq (5) ans.

8. Entrée en vigueur

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration, soit le 29 novembre 2017.

NOTE : *Dans la présente politique, sauf usage contraire en langue française, le masculin est utilisé comme genre épicène.*

ANNEXE 1

Article 7.1

Règlement numéro 12 : Règlement sur l'utilisation des technologies informatiques et internet

L'article 7.1 du *Règlement numéro 12* : *Règlement sur l'utilisation des technologies informatiques et internet* est applicable tant pour l'informatique que l'information.

7.1. PROCÉDURE D'ENQUÊTE ET DE SURVEILLANCE

Le comité d'enquête est composé de trois (3) personnes : un membre de l'équipe de la direction des ressources humaines, un membre de l'exécutif syndical concerné ou association représentante et un membre de la direction. Le choix des membres du comité d'enquête est fait de façon à assurer la crédibilité du processus d'enquête.

Le comité d'enquête doit, dans un premier temps, déterminer les moyens d'enquête utilisés de même que l'étendue de la surveillance en lien avec ladite situation.

Lorsqu'il le juge nécessaire, le comité d'enquête peut convenir, de façon unanime, de s'adjoindre la collaboration d'une personne-ressource dont l'expertise est susceptible d'aider le comité dans la conduite de son enquête.

Toute enquête en application de ce règlement est traitée de façon confidentielle tant qu'elle n'est pas complétée et que les suites appropriées n'ont pas été apportées.

Les dossiers constitués en application de ce règlement sont confidentiels et ne sont accessibles qu'aux personnes suivantes :

- la direction des ressources humaines;
- les membres du comité de direction du Collège;
- les membres du comité d'enquête;
- exécutif syndical ou exécutif de l'association représentante.

Une fois l'enquête terminée, le comité d'enquête rédige son rapport d'enquête dans lequel il consigne :

- les faits à l'origine de la situation faisant l'objet de l'enquête;
- les principales étapes de son enquête (méthodologie);
- la liste des personnes rencontrées dans le cadre de l'enquête;
- la documentation examinée;
- un résumé des faits révélés par l'enquête;
- l'analyse;
- les conclusions.

Au terme du processus d'enquête, la direction des ressources humaines détermine les suites à donner.