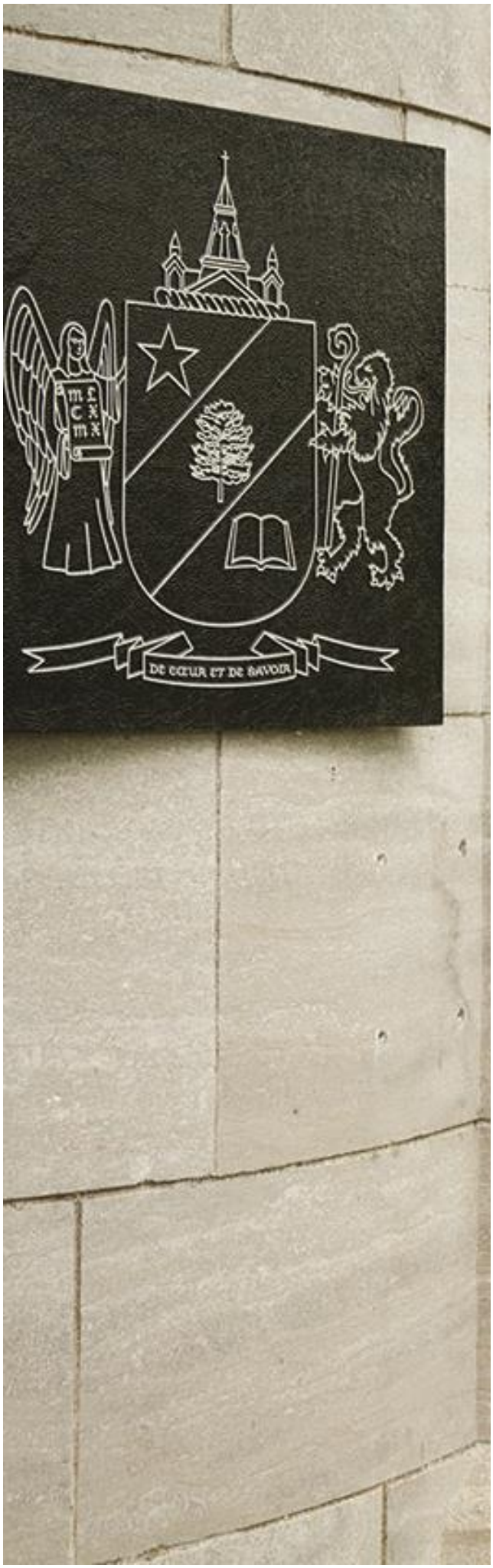


cegep de Saint-Jérôme
SAINT-JÉRÔME
MONT-TREMBLANT
MONT-LAURIER

# DIRECTIVE DU COMITÉ DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (CAIPRP)

## Sous-comité du comité de sécurité de l'information

**Adoptée par le comité de direction le 11 octobre 2022**

SECRÉTARIAT GÉNÉRAL
ET AFFAIRES JURIDIQUES
CÉGEP DE SAINT-JÉRÔME
Saint-Jérôme | Mont-Tremblant | Mont-Laurier

# TABLE DES MATIÈRES

**PRÉAMBULE** ..... **4**

**CHAMPS D'APPLICATION** ..... **4**

**CADRE LÉGAL** ..... **4**

**MANDAT** ..... **4**

**COMPOSITION** ..... **5**

**RESPONSABILITÉS ET FONCTIONS** ..... **5**

**PROJET DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES** ..... **6**

**FONCTIONNEMENT** ..... **8**

# PRÉAMBULE

Le Cégep de Saint-Jérôme (ci-après le Collège) est responsable de la protection des renseignements personnels qu'il détient, et ce, même s'ils sont hébergés par un tiers. En vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, le Collège doit mettre sur pied un comité d'accès à l'information et de protection des renseignements personnels (ci-après le CAIPRP) qui veillera notamment à mettre en place une gouvernance priorisant la confidentialité de l'information relative à la vie privée.

# CHAMPS D'APPLICATION

La présente directive s'applique à l'égard de tout renseignement personnel détenu par le Collège dans l'exercice de ses fonctions, notamment celles en enseignement et en recherche, que sa conservation soit assurée par le Collège ou par un tiers. Elle s'applique à toute personne liée au Collège en tant que membre de la communauté collégiale et s'étend également à tout fournisseur ou partenaire du Collège, incluant les sous-traitants, ayant accès à un renseignement personnel détenu par le Collège.

# CADRE LÉGAL

- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels
- Code civil du Québec
- Politique sur la sécurité de l'information
- Directive sur l'utilisation de l'infonuagique

# MANDAT

Afin de répondre aux exigences de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* le CAIPRP, sous-comité du Comité de sécurité de l'information (CSI) a été créé afin de soutenir le Collège dans l'exercice de ses responsabilités et dans l'exécution de ses obligations, notamment en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. À cette fin, une charte définissant le mandat et les fonctions de ce comité avait été adoptée et les éléments de celle-ci se retrouvent dans la présente Directive.

# COMPOSITION

Le sous-comité est composé des personnes occupant les fonctions suivantes ou de la personne déléguée au sein de leur Direction/Service.

- Personne responsable de l'accès à l'information et de la protection des renseignements personnels
    - Secrétaire générale
- Responsable de la sécurité de l'information (RSI)
    - Direction responsable
- Personne ayant accès, de par ses fonctions, à de nombreux renseignements personnels
    - Direction des ressources humaines
    - Registraire
    - Coordination du Service des ressources des technologies de l'information
    - Analyste en gestion de l'information et des archives
    - Coordination de la Direction de la vie étudiante (Carrefour d'aide aux étudiants)

Le CAIPRP peut inviter ponctuellement toute autre personne possédant une expertise pertinente afin de l'assister dans la réalisation de son mandat. Toutefois, ces invités ne possèdent aucun droit de vote.

# RESPONSABILITÉS ET FONCTIONS

Comme son titre l'indique, la loi consacre deux responsabilités distinctes à ce comité, celle de l'accès aux documents et celle de la protection des renseignements personnels.

- Soutenir la personne responsable de l'accès et la protection des renseignements personnels dans l'exercice de ses responsabilités et dans l'exécution de ses obligations
- évaluer les facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels (art. 63.5)
- Recommander pour adoption les règles de gouvernance sur l'accès à l'information et la protection des renseignements personnels
    - Rôles et responsabilités du personnel « tout au long du cycle de vie » des renseignements personnels.
    - Processus de traitement internes des plaintes
    - Description des activités de formation et de sensibilisation offertes au personnel

    - Mesures de protection à l'égard des sondages
- S'assurer que les règles approuvées par le comité de direction sont publiées
- Rédiger une Politique de confidentialité en termes simples et clairs (art. 63.4)
- Utiliser des moyens qui assurent la protection des renseignements personnels dès leur conception (art. 63.7) (Privacy by design)
- En cas d'incident de confidentialité[1] présentant un risque de préjudice sérieux, obligation d'aviser :
    - La Commission d'accès à l'information (CAI)
    - La personne concernée.

# PROJET DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES

Dès le début d'un projet d'acquisition, de développement et de refonte de systèmes d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels, le CAIPRP doit être consulté aux fins de l'évaluation des facteurs relatifs à la vie privée. Les mises à jour de tels systèmes sont exclues de la consultation, mais si la mise à jour d'un système d'information ou d'une prestation électronique de services a une incidence importante sur la protection des renseignements personnels, le CAIPRP est consulté aux fins de l'évaluation des facteurs relatifs à la vie privée.

Les projets visés concernent, entre autres, des bases de données, des logiciels d'application, des vidéos de surveillance.

L'évaluation des facteurs relatifs à la vie privée est une démarche préventive qui vise à mieux protéger les renseignements personnels et à respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui entraîneraient des conséquences positives et négatives sur le respect de la vie privée des personnes concernées.

[1] La loi définit l'incident de confidentialité comme étant l'accès non autorisé par la loi à un renseignement personnel, l'utilisation ou la communication non autorisée par la loi d'un tel renseignement, la perte de ce renseignement ou toute autre atteinte à sa protection. Cet incident, impliquant des renseignements personnels, représente un risque sérieux d'atteinte à la vie privée d'un membre de la communauté collégiale.

Ces facteurs sont :

- la conformité d'un projet avec la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient ;
- la détermination des risques d'atteinte à la vie privée engendrés par ce projet et l'évaluation de leurs conséquences ;
- la mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

Lorsqu'il est consulté à ce sujet, le CAIPRP doit tenir compte que la réalisation de cette évaluation doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

À toute étape d'un projet de conception d'un système d'information ou de prestation électronique de services, le CAIPRP peut suggérer des mesures de protection des renseignements personnels applicables à ce projet telles que :

1. la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels ;
2. des mesures de protection des renseignements personnels dans tout document relatif au projet, tel qu'un cahier des charges ou un contrat ;
3. une description des responsabilités des participants au projet en matière de protection des renseignements personnels ;
4. la tenue d'activités de formation sur la protection des renseignements personnels pour les personnes participantes au projet.

Le CAIPRP peut déterminer des catégories de projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services et prévoir pour chacune de ces catégories les modalités d'évaluation des facteurs relatifs à la vie privée. Pour chaque catégorie déterminée, un sous-comité possédant une expertise pertinente sur la question reçoit l'évaluation effectuée et au besoin, traite dans les meilleurs délais toute problématique reliée à cette évaluation. Ce sous-comité s'adjoint toute personne invitée dont l'expertise est requise. Le compte rendu des délibérations de chaque sous-comité est déposé lors de la prochaine réunion du CAIPRP.

De plus, la secrétaire générale ou le secrétaire général met en place un processus flexible pour assurer la progression des dossiers d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services en dehors des rencontres du CAIPRP ou d'un de ses sous-comités.

# FONCTIONNEMENT

1. Le comité doit tenir un minimum de deux (2) réunions par année.
2. Le quorum est fixé à la majorité des membres présents.
3. Le plan de travail du CAIPRP est intégré à celui du Comité de sécurité de l'information (CSI).
4. Un compte rendu des réunions est déposé au CSI et acheminé à la direction générale.
5. Le Secrétariat général pourvoit au soutien et au secrétariat du comité.
6. Le comité révise tous les cinq (5) ans, ou plus tôt au besoin, son mandat ainsi que ses responsabilités et fonctions et rend compte au CSI et lui transmet toute recommandation de modification.