# DIRECTIVE SUR L'ACCÈS AUX SYSTÈMES INFORMATIQUES ET LE TRANSPORT DE MATÉRIEL HORS CANADA

- Adoptée le 11 mai 2026 en comité de direction

**Direction des technologies de l'information**

CÉGEP SOREL TRACY

# TABLE DES MATIÈRES

## Cadre réglementaire :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (**LGGRI**)

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*

- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (**Loi 25**)

## Définitions :

- **Cégep / Collège**: Cégep de Sorel-Tracy et son Campus de Varennes.

- **CSIO :** Chef de la sécurité de l'information organisationnelle. (Cette fonction est actuellement assumée par la direction des technologies de l'information).

- **Lieu habituel de travail** : endroit où un membre du personnel effectue habituellement ses tâches.

- **Réseau sécurisé** : infrastructure mise en place pour protéger la confidentialité, l'intégrité et la disponibilité des données et des ressources. Il garantit que les accès non autorisés, les violations de données et les activités malveillantes sont évités ou réduits au minimum, peu importe l'origine de la connexion.

  Il protège les informations qui circulent entre un appareil, système ou autres et Internet. Il assure à l'usager ou l'usagère ainsi qu'au Cégep un contrôle sur l'infrastructure réseau, pares-feux, etc.

  ** La règle de base est de ne jamais présumer de la confiance d'un réseau ou de l'environnement sur lequel l'usager ou l'usagère est connecté(e).*

- **MCN** : ministère de la Cybersécurité et du numérique.

- **Télétravail** : régime de travail souple selon lequel la personne employée a l'autorisation d'effectuer ses tâches dans un lieu extérieur à son lieu habituel de travail, au Canada, au moyen de technologies de l'information et des communications (TIC), en respect de l'horaire de travail établi, de la *Politique de sécurité de l'information* du Cégep et de la *Loi 25*.

## 1. Préambule

À la suite de la mise en place des nouvelles mesures de sécurité du ministère de la Cybersécurité et du Numérique (MCN) et de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (*Loi 25)*, le Cégep met en place les règles à suivre concernant l'accès aux systèmes informatiques de l'établissement et le transport de matériel hors Canada.

L'accès aux systèmes informatiques du Collège hors du Canada a des répercussions importantes sur la sécurité informatique, la confidentialité, la disponibilité et l'intégrité des données, la protection des renseignements personnels ainsi que la capacité des services informatiques à offrir le support adéquat aux usagers et usagères.

La présente *Directive sur l'accès aux systèmes informatiques et le transport de matériel hors Canada* s'inscrit dans le cadre de l'application de la *Politique de sécurité de l'information* et du *Cadre gouvernemental de gestion de la sécurité de l'information* émis par le MCN conformément à la *Loi sur la gouvernance et la gestion informationnelles des organismes publics et des entreprises du gouvernement* (**LGGRI**).

Elle découle des différentes obligations légales qui sont dévolues au Cégep, tel que la *LGGRI*, la *Loi 25*, la *Politique de sécurité de l'information* ainsi que des lois de pays étrangers. Elle s'applique en respect des différents règlements, politiques et directives du Collège.

## 2. Objectifs

Le Cégep, en mettant en place la présente *Directive*, entend poursuivre les objectifs suivants :

- fournir des balises claires et précises pour l'accès et le transport d'équipement hors Canada;
- offrir au personnel admissible la possibilité d'effectuer leurs tâches dans le cadre d'un voyage professionnel autorisé;
- que le service des technologies de l'information soit en mesure d'agir rapidement dans le cas de situation imprévisible, d'urgence, de fuite de données, de vol de mot de passe, etc.

## 3. Champ d'application

La présente *Directive* s'applique à l'ensemble des membres de la communauté collégiale.

## 4. Interdiction

Il est formellement interdit à tout membre de la communauté collégiale d'accéder aux systèmes informatiques de l'établissement, aux données étudiantes (CLARA, Omnivox ou autres plateformes), aux renseignements personnels et aux informations confidentielles depuis un emplacement situé à l'extérieur des frontières canadiennes, notamment, dans le cadre de :

- vacances et congés;
- voyages professionnels, à moins d'autorisation spécifique (article 5);
- prestation de travail effectuée depuis une juridiction étrangère.

Le matériel informatique mis à la disposition des usagers et usagères par le Cégep ne doit pas être transporté et utilisé hors du Canada afin de minimiser les risques liés à la sécurité de l'information, la sécurité des données personnelles, l'intégrité et la confidentialité des données. Il

est également interdit d'effectuer toute copie ou sauvegarde de données sensibles, et ce, dans l'objectif de travailler à l'extérieur du Canada.

## 5. Exigences d'approbation

Pour qu'un usager ou une usagère soit autorisé(e) à accéder aux systèmes informatiques et/ou à transporter du matériel informatique du Cégep hors Canada, les éléments suivants doivent être respectés :

- la demande doit s'inscrire dans le cadre d'un déplacement professionnel autorisé par son ou sa gestionnaire, quelle que soit la durée;
- avoir la confirmation que le lieu où la prestation de travail sera effectuée respecte les lois et règlements en vigueur au Québec ainsi que les recommandations des différentes instances en cybersécurité (MCN, Centre canadien pour la cybersécurité, etc.);
- s'assurer que le lieu où sera effectuée la prestation de travail permet de préserver la confidentialité des données ainsi que la protection des renseignements personnels *(Loi 25)*;
- disposer d'une connexion au réseau sécurisé, par exemple, éviter les accès offerts gratuitement comme les hôtels, aéroports et cafés;
- disposer d'une connexion au réseau Internet de bonne qualité permettant l'exécution des tâches, pouvant ainsi permettre la tenue de visioconférences adéquates.

L'évaluation de ces éléments relève de la direction des technologies de l'information. Toute autorisation d'accès informatique hors Canada peut être révoquée en tout temps si la personne ou la situation ne répond plus à l'un des critères d'admissibilité ou si des problématiques de sécurité surviennent, notamment, en raison d'alerte de cybersécurité ou sur recommandation d'une firme experte ou d'évènement susceptible de porter atteinte au Collège.

Dans ce cas, l'usager ou l'usagère ayant bénéficié(e) d'une autorisation conformément à la présente *Directive*, devra immédiatement se conformer et prendre toutes les mesures nécessaires en lien avec le retrait de ladite autorisation.

## 6. Responsabilités

### 6.1 Responsabilités de la direction des technologies de l'information

- Veiller à l'application de la présente *Directive* ainsi que sa mise à jour.
- Fournir le soutien technique adéquat sous réserve de ce qui est réalisable dans un Contexte où le service à rendre est à distance.
- S'assurer que l'usager ou l'usagère confirme que le lieu où est effectué sa prestation de travail est conforme aux différentes normes de sécurité informatique.
- Effectuer une surveillance en continu afin de mitiger les risques.

### 6.2 Responsabilités du ou de la gestionnaire

- S'assurer de l'application de la présente *Directive* dans son service.
- Assumer toute autre responsabilité découlant de l'application de la présente *Directive*.

### 6.3 Responsabilités de l'usager ou de l'usagère

- S'assurer que l'ensemble des critères d'admissibilité ayant permis l'accès aux systèmes et le transport de matériel informatique hors Canada soient respectés, et ce, pour toute la durée où l'autorisation est octroyée, tel que prévu à l'article 5.
- S'assurer de l'utilisation sécuritaire des données informatiques.

- Se conformer en tout temps aux règlements et politiques du Collège, tel que la *Politique de confidentialité* et la *Politique de sécurité de l'information*.
- Aviser immédiatement la direction des technologies de l'information de tout bris, panne ou autre situation l'empêchant d'effectuer sa prestation de travail ou de toute problématique liée à la sécurité de l'information.
- Déclarer sans délai au ou à la responsable de la protection des renseignements personnels tout incident pouvant mener à une fuite de données ou à un incident de confidentialité conformément à la *Loi 25*.
- Utiliser à des fins professionnelles exclusivement le matériel et les systèmes informatiques du Cégep, à moins d'autorisation explicite de la direction des technologies de l'information.

## 7. Responsabilités non liées à l'emploi

Le transport du matériel informatique et l'accès aux systèmes informatiques hors Canada ne peuvent servir dans le cadre de voyage personnel, de congé ou de vacances. De même l'usager ou l'usagère ne doit en aucun cas transporter de matériel informatique ou utiliser des applications tierces ou non autorisées aux fins de déjouer les systèmes de sécurité du Collège.

## 8. Sécurité et confidentialité des données

Tous les documents, les équipements et les informations utilisés par un usager ou une usagère à l'extérieur des lieux habituels de travail doivent être conservés en toute sécurité et de manière confidentielle. La personne employée doit également s'assurer qu'ils ne sont pas accessibles à d'autres personnes. Pour ce faire, l'utilisation d'un espace de travail dédié à la personne employée est requise. La *Politique de sécurité de l'information* et la *Loi 25* se doivent d'être respectées, comme si la personne était sur le lieu habituel de travail.

À défaut de faire preuve de prudence dans la sauvegarde des informations confidentielles et exclusives au Cégep dans toutes les phases de possession (transport, utilisation, stockage et élimination), l'accès aux systèmes en dehors du Canada sera résilié et des mesures administratives ou disciplinaires pourraient être prises.

## 9. Fournitures, équipements et outils

Le Cégep ne fournira pas d'équipement de bureau ou de matériel informatique additionnel à celui déjà fourni sur le lieu habituel de travail afin de permettre le travail hors Canada. Il est de la responsabilité de l'usager ou de l'usagère de disposer d'une connexion Internet de qualité et sécuritaire.

L'usager ou l'usagère doit s'assurer de maintenir en bon état le matériel que le Cégep met à sa disposition et est responsable des dommages qui y sont causés, autrement que par l'usure normale. Celui-ci demeure en tout temps la propriété du Collège. Ainsi, il doit servir à des fins professionnelles exclusivement et non pour un usage personnel.

L'usager ou l'usagère autorisé(e) à accéder aux systèmes informatiques et/ou à transporter du matériel informatique du Cégep hors Canada conformément à la présente *Directive*, pourra avoir accès à un service technique à distance, sous réserve du support qui peut être apporté dans ce contexte, et ce, en soumettant une requête via *Octopus*.

## 10. Entrée en vigueur de la directive et révision

La présente *Directive* entre en vigueur le jour de son adoption par le comité de direction. Elle est sujette à révision au besoin.