Directive de gestion des identités et des accès
Numéro D-28

Adoption (instance/autorité)	*Date*	*Résolution*
Comité de direction	Le 27 mai 2025	
Modification (instance/autorité)	*Date*	*Résolution*
Abrogation (instance/autorité)	*Date*	*Résolution*

Entrée en vigueur	Le 27 mai 2025
Responsable de l'application	Direction des services administratifs
Historique	

TABLE DES MATIÈRES

1 ÉNONCÉ DE PRINCIPE

En assurant un contrôle efficace des accès à l'information, le Cégep de Matane réduit les risques encourus à l'égard des objectifs d'intégrité, de disponibilité et de confidentialité de son information, ainsi que de la protection des renseignements personnels.

La *Directive de gestion des identités et des accès* définit les lignes directrices en matière de gestion des accès et les responsabilités à assumer par les principales personnes intervenantes, notamment la personne dirigeante de l'organisme, la personne cheffe de la sécurité de l'information organisationnelle (CSIO), la personne en charge de la coordination organisationnelle des mesures de sécurité de l'information (COMSI), les personnes détentrices de l'information, les personnes gestionnaires des unités administratives, la personne responsable du Service des ressources informationnelles, la personne administratrice des accès, et les personnes utilisatrices.

Elle précise également les sanctions prévues pour toute personne utilisatrice qui contrevient aux dispositions énoncées.

2 CHAMP D'APPLICATION

La présente Directive s'applique à :

- L'information que détient l'organisme dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers;
- L'information confiée à l'organisme en vertu d'une entente et qui est reconnue comme devant faire l'objet d'un contrôle d'accès;
- Les informations personnelles;
- L'infrastructure technologique de l'organisme;
- Toute personne physique ou morale qui, à titre de personne employée, consultante, stagiaire, partenaire ou fournisseur, a un accès, sur place ou à distance, à l'information dont la sécurité est assurée par l'organisme.

3 CADRE LÉGAL ET ADMINISTRATIF

- *Loi sur les collèges d'enseignement général et professionnel (chapitre C-29);*
- *Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);*
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);*
- *Loi sur les archives (chapitre A-21.1);*
- *Loi sur la protection des renseignements personnels;*
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);*
- *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels;*
- *Directive sur la sécurité de l'information gouvernementale, en vigueur depuis le 8 décembre 2021;*
- *Cadre gouvernemental de gestion de la sécurité de l'information, en vigueur depuis le 15 janvier 2014;*
- *Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information;*

- *Politique gouvernementale de cybersécurité (axe 2, objectif 3);*
- *Arrêté numéro 2022-03 du ministre de la Cybersécurité et du Numérique en date du 23 juin 2022 (articles 17 et 18 relatifs à la sécurité de l'information);*
- *Politique sur la sécurité de l'information (P-36).*

4 DISPOSITIONS GÉNÉRALES

4.1 LIGNES DIRECTRICES DE LA GESTION DES ACCÈS

La documentation nécessaire à la mise en place du processus formel de gestion des accès doit être élaborée et révisée, lorsque requis.

Les accès à l'information doivent être définis sur la base du principe du moindre privilège et du principe de séparation des tâches.

Un compte unique et nominatif est requis pour chaque accès octroyé. Les comptes génériques doivent être évités, à moins d'en justifier techniquement l'utilisation et de le documenter dans le cadre d'une dérogation.

L'octroi et l'utilisation de privilèges (comptes à privilèges spéciaux) doivent être encadrés et contrôlés rigoureusement et être approuvés par la personne CSIO.

Les justificatifs d'attribution des privilèges d'accès de haut niveau doivent rester valides durant toute la période d'attribution de ces privilèges et devront être documentés dans un billet C2.

Le départ, le transfert ou la mutation d'une personne utilisatrice ainsi que tout autre changement relatif à ses tâches et ses fonctions doit conduire systématiquement à la révision de ses droits d'accès.

Les accès temporaires et/ou exceptionnels doivent être autorisés par la personne gestionnaire et la personne détentrice concernée.

Les accès attribués doivent être revus deux fois par an. Les droits, leurs modifications et leurs violations doivent être répertoriés.

Les équipements informatiques de l'organisme doivent être protégés adéquatement contre tout accès non autorisé et contre toute perte ou tout dommage qui pourrait être causé de façon accidentelle ou délibérée.

L'attribution d'un accès à des données stratégiques est précédée d'un engagement formel de la personne utilisatrice (entente de confidentialité) quant au respect des règles de protection des moyens d'accès fournis et au devoir de signalement en cas de divulgation non autorisée ou même de suspicion de divulgation d'information stratégique.

4.2 SANCTIONS

Lorsqu'une personne utilisatrice contrevient à la présente directive ou aux réglementations en découlant, elle s'expose à des mesures disciplinaires, administratives ou légales en fonction de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

L'organisme peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise.

5 RESPONSABILITÉS

Dans le cadre de la mise en place d'un processus formel de gestion des accès, les principales responsabilités assignées par la présente directive sont les suivantes :

Le comité de direction

- Approuve la présente directive et en assure la diffusion.

La personne cheffe de la sécurité de l'information organisationnelle (CSIO)

- S'assure de la mise en place du processus formel de gestion des accès à l'information au sein de son organisme;
- Élabore et met à jour la présente Directive et la soumet pour validation au comité de direction;
- Dirige le processus de gestion des identités et des accès;
- S'assure de la documentation et de la mise à jour des procédures nécessaires à la mise en place du processus formel de gestion des identités et des accès;
- S'assure de la mise en œuvre du processus de gestion, de révision des accès et des contrôles associés;
- S'assure qu'un audit des mécanismes de contrôle de gestion des identités et des accès (bilan de sécurité et reddition de comptes) est effectué deux (2) fois par an et transmis aux personnes responsables de systèmes;
- S'assure que des séances de sensibilisation aux risques de sécurité soient offertes aux personnes utilisatrices;
- Approuve toute dérogation et les documente aux dispositions de la directive.

La personne en charge de la coordination organisationnelle des mesures de sécurité de l'information (COMSI)

- Contribue à l'élaboration, la mise en œuvre et la révision de la présente Directive;
- Détermine les menaces et les situations de vulnérabilité liées à la gestion des identités et des accès et, si requis, propose des mesures de renforcement des contrôles d'accès;
- Formule des avis de pertinence sur les mécanismes de gestion des accès mis en place.

Les personnes détentrices de l'information

Les personnes détentrices de l'information sont désignées par la personne CSIO. Leurs noms et les systèmes d'information qui leur sont assignés sont consignés au registre d'autorité. Parmi leurs responsabilités, elles :

- Définissent les listes de droits à assigner – profils d'accès applicatifs – supportées par les systèmes de mission relevant de leur autorité et s'assurent de la conformité des mécanismes d'accès aux exigences relatives à la sécurité de cette information;
- Définissent les accès à l'information sur la base du principe du moindre privilège et du principe de la séparation des tâches;
- Autorisent les accès à l'information relevant de leur autorité;
- Participent à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans en matière de sécurité de l'information;
- Catégorisent l'information relevant de leur responsabilité en fonction de sa valeur et selon les critères de disponibilité, d'intégrité et de confidentialité;
- Veillent à ce que les mesures de sécurité de l'information adoptées soient mises en place et appliquées et qu'elles répondent adéquatement aux risques encourus, incluant la gestion des accès;
- Agissent comme maîtres d'œuvre des analyses de risques et s'assurent de la prise en charge des risques résiduels;
- Veillent au respect du registre d'autorité par les personnes utilisatrices qui relèvent de leur responsabilité.

Les personnes gestionnaires

- Définissent les listes de droits à assigner – les habilitations et les critères d'habilitation – associées aux fonctions organisationnelles relevant de leur autorité;
- S'assurent de la conformité, en tout temps, des accès autorisés au principe du privilège minimal et des qualifications de leur personnel aux critères d'habilitation associés aux fonctions occupées;
- Documentent les processus d'affaires et définissent clairement les règles de séparation des tâches associées;
- Autorisent et justifient tout besoin d'accès à l'information qui ne fait pas partie des permissions prévues pour la fonction occupée par l'employé;
- Assurent le suivi des autorisations d'accès octroyées aux personnes utilisatrices relevant de leur autorité depuis leur arrivée jusqu'au départ de leur unité administrative;
- Ajustent dans les délais recommandés tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès réellement octroyées;
- S'assurent de l'intégration dans les ententes et contrats de clauses garantissant le respect des exigences en matière de sécurité de l'information, dont celles sur la gestion des accès.

La personne responsable de la gestion des technologies de l'information

- Met en place les solutions technologiques répondant aux exigences de la présente Directive;
- Met en place les outils de journalisation des accès, permettant ainsi, lors des vérifications périodiques ou sur demande, de savoir qui a accédé à quoi;
- S'assure que les personnes utilisatrices n'ont pas accès à leur poste de travail en tant que personne administratrice, et que toute exception est documentée et approuvée;
- Met en place sur les postes de travail des mesures de protection contre les accès non autorisés et les vulnérabilités logicielles;
- Met en place les mécanismes de surveillance des méthodes d'accès à distance.

La personne administratrice des droits d'accès

- Applique la présente Directive et les procédures afférentes;
- Crée les identifiants et les droits d'accès pour les personnes utilisatrices dûment autorisées par les personnes gestionnaires et les personnes détentrices de l'information;
- Édite à l'intention des personnes détentrices de l'information et des personnes gestionnaires les rapports des autorisations d'accès réellement attribuées, et s'assure de leur validation.

La personne utilisatrice

- N'emploie l'information à laquelle elle a accès que pour des tâches qui lui sont assignées;
- Est responsable des accès qui lui sont octroyés, et est redevable auprès de ses personnes gestionnaires de toute action exécutée en utilisant son identifiant et son authentifiant;
- S'engage formellement au respect des règles de protection des moyens d'accès aux données stratégiques;

6 ENTRÉE EN VIGUEUR ET DIFFUSION

La présente Directive entre en vigueur au moment de son adoption par le comité de direction. La Direction des services administratifs diffuse cette Directive auprès de la communauté collégiale.

7 CALENDRIER DE RÉVISION

Cette Directive peut être révisée à tout moment. Toutefois, une révision est prévue trois (3) ans à compter de la date de son adoption.