Directive sur la gestion des identités et des accès en ressources informationnelles

En vigueur le 18 juin 2025

Note importante :

Une procédure interne à accès restreint liée à la présente Directive est rendue disponible aux membres du personnel cadre et au personnel de la Direction des technologies de l'information. Voir les détails à l'article 6 ci-après.

Lien pour accéder à la procédure interne correspondante.

1. Préambule

En tant qu'organisme public, le Cégep doit encadrer et contrôler la gestion des identités et des accès (GIA) à ses actifs informationnels pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le Cégep soient strictement réservés aux personnes autorisées afin d'en assurer une utilisation sécuritaire.

En d'autres mots, la GIA assure l'équilibre entre la protection de l'information que l'organisme détient et l'octroi des accès et des privilèges aux personnes utilisatrices pour qu'elles puissent travailler efficacement.

La présente Directive découle de la Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information et est une composante du Cadre de gestion de la sécurité des technologies de l'information.

2. Objectifs

La présente Directive vise à :

- encadrer l'attribution des comptes utilisateurs et des accès aux actifs informationnels du Cégep permettant l'utilisation du réseau, des systèmes et des données, et ce, en conformité avec les règles de sécurité en vigueur;
- identifier les personnes ayant un rôle dans le processus d'attribution des accès et définir ces rôles;
- assurer l'efficacité et la rapidité dans l'attribution et la gestion des droits et privilèges aux personnes utilisatrices, le tout en accord avec les normes du domaine de la GIA, notamment la norme ISO/IEC 27001:2022.

3. Champ d'application

La présente Directive s'applique à toute personne physique ayant accès, sur place ou à l'extérieur des locaux du Cégep, aux actifs informationnels pour lesquels le Cégep a la responsabilité d'assurer la sécurité et la gestion.

Elle concerne la gestion des autorisations et des accès en fonction du statut de la personne utilisatrice et, dans le cas d'un membre du personnel ou d'un partenaire, des exigences liées à ses fonctions.

4. Définitions

Un lexique des termes utilisés en ressources informationnelles (RI) est rendu disponible sur la plateforme Axel.TI (Omnivox) dans la section « Lexique ».

5. Principes de gestion

L'octroi d'accès et de privilèges aux actifs informationnels est réalisé en conformité avec deux principes de gestion :

1. L'attribution en fonction du droit d'accès minimal :

   > Droit d'accès restreint de manière à ce que la personne utilisatrice puisse n'accomplir avec celui-ci que les seules tâches autorisées et nécessaires à l'exercice de ses fonctions (source : Office québécois de la langue française).

2. L'attribution selon le principe de confiance zéro :

   > Les droits et privilèges sont vérifiés de façon systématique et attribués selon les rôles occupés par la personne utilisatrice sans égard à l'identité ou la réputation de celle-ci.

6. Gestion des accès selon le type de compte

Le document intitulé « Procédure pour personnel d'encadrement - Gestion des identités et des accès en ressources informationnelles » est rendu disponible au personnel cadre (et aux personnes qu'elles auront déléguées, le cas échéant) ainsi qu'au personnel de la Direction des technologies de l'information (DTI). Ces deux groupes jouent un rôle clé dans la mise en application de la présente Directive.

6.1 Membres du personnel

6.1.1 Embauche : création d'un nouveau compte

La Direction des ressources humaines (DRH) est responsable de soumettre une requête à la Direction des technologies de l'information (DTI) contenant les informations ayant trait à l'embauche d'un nouveau membre du personnel afin que les accès de base soient attribués (compte Microsoft, espaces de stockage et licence Microsoft Office).

La coordination ou la direction de la nouvelle ressource doit soumettre une requête demandant les droits d'accès aux logiciels de gestion en fonction du poste de la nouvelle personne. Des validations de conformités seront effectuées par la DTI et des autorisations pourraient être demandées aux responsables concernés avant l'attribution des droits.

6.1.2 Absence prolongée et retour au travail : suspension et réactivation du compte

La DRH est responsable de transmettre à la DTI les informations ayant trait aux dates de départ et de retour de la personne utilisatrice afin que les accès soient suspendus ou réactivés.

Les accès aux logiciels de gestion sont automatiquement suspendus au début du congé.

Dans le cas d'une absence prolongée supérieure à trois (3) mois, le niveau d'accès aux services Microsoft 365 sera réduit pour ne permettre que l'accès à la boîte courriel. Une demande de rapatriement du portable à la DTI pourrait également être faite.

Au retour de la personne utilisatrice, la coordination ou la direction responsable doit soumettre une requête demandant les droits d'accès aux logiciels de gestion ainsi que les accès Microsoft 365 en fonction des tâches assignées à la ressource.

Des validations de conformités seront effectuées par la DTI et des autorisations pourraient être demandées aux responsables concernés avant l'attribution des droits.

6.1.3 Changement de fonction

La coordination ou la direction accueillant une nouvelle ressource doit soumettre une requête (Mouvement de personnel) à la DTI pour signaler un changement de fonction et demander les droits d'accès aux logiciels de gestion et aux espaces de stockage de l'unité en fonction du poste occupé.

Selon le cas, cette requête devra tenir compte d'un plan de transition (maximum 30 jours) convenu avec la coordination ou la direction d'où provient la personne utilisatrice.

Des validations seront effectuées par la DTI avant l'attribution des droits demandés.

Si, dans le cadre d'un plan de transition, il est nécessaire de permettre à une personne d'avoir accès aux comptes de deux fonctions différentes simultanément pour fins de formation, la DTI recommande d'utiliser uniquement l'accès de la nouvelle ressource, et ce, afin de réduire les risques de sécurité.

Selon la situation, la DTI pourra convenir d'un accommodement avec la coordination ou la direction concernée.

La DTI s'assurera de fermer les accès liés à l'ancien poste de la ressource dans les délais convenus.

6.1.4 Fin d'emploi définitive : suspension du compte

La DRH est responsable de soumettre une requête à la DTI l'avisant de la date de départ de la personne utilisatrice (démission, retraite, fin de priorité d'emploi, congédiement ou décès) afin que les accès soient désactivés. Les accès de base (compte réseau et espaces de stockage du secteur) seront désactivés à la fin de la dernière journée de travail.

Dans le cas d'une démission ou d'une retraite, la personne utilisatrice (et sa coordination ou sa direction) recevra un courriel l'invitant à déplacer les données pertinentes (incluant les courriels) vers les espaces de stockage de sa coordination ou direction. La boîte courriel et l'espace de stockage personnel devront être vides à son départ. Une réponse automatique d'absence dans la boîte courriel devra être activée par la personne utilisatrice.

Dans le cas d'un congédiement ou d'un décès, un membre de la DTI activera un message d'absence dans la boîte courriel.

Message suggéré :

> Veuillez noter que je ne serai plus à l'emploi du Cégep de Sherbrooke à compter du AAAA/MM/JJ, veuillez transmettre votre courriel à la personne qui assumera le suivi à mon départ, soit :
>
> M. Mme Nom, adresse courriel
>
> Merci.

La personne utilisatrice ne pourra pas récupérer les données après son départ.

6.2 Membres de la communauté étudiante

6.2.1 Inscription : création d'un nouveau compte

Les accès de base (compte réseau et espace de stockage personnel) sont automatiquement attribués au moment de l'inscription de la personne étudiante.

Un délai de deux (2) jours ouvrables pourrait être nécessaire dans le cas d'une inscription tardive.

6.2.2 Changement de programme

Les accès de la personne étudiante qui change de programme ou de cours seront modifiés automatiquement au moment de la mise à jour du dossier par le Service de l'organisation scolaire, du registrariat et de l'aide pédagogique (SOSRAP).

6.2.3 Fin du parcours scolaire et suspension temporaire

Les accès de la personne étudiante qui met fin à son parcours scolaire seront modifiés automatiquement au moment de la mise à jour du dossier par le SOSRAP.

Dans le cas d'une suspension administrative d'une personne étudiante, le SOSRAP doit transmettre sans délai l'information à la DTI.

La personne étudiante qui quitte définitivement et qui ne prévoit pas s'inscrire à la session suivante doit récupérer le contenu de son espace de stockage et de sa boîte courriel au plus tard le dernier jour de la session active. Une fois la session terminée, le contenu sera supprimé sans préavis et ne pourra pas être récupéré.

6.3 Partenaires

Une personne est considérée comme « partenaire » si elle collabore de près aux activités du Cégep sans être membre du personnel ou de la communauté étudiante. Elle peut notamment

être : membre du personnel de la Coop du Cégep, stagiaire, membre du personnel de la Fondation Cégep de Sherbrooke, une ressource consultante, une personne provenant d'une firme de vérification, une personne accompagnatrice en services adaptés d'un organisme externe, etc.

Ces partenaires sont sous la responsabilité d'une personne cadre qui veille à les informer des dispositions et exigences de la présente Directive.

La liste des responsables est disponible sur la plateforme Axel.TI (Omnivox).

6.3.1 Arrivée d'un partenaire : création d'un nouveau compte

La personne cadre identifiée comme responsable du partenaire doit soumettre une requête à la DTI contenant les informations ayant trait à l'arrivée d'un nouveau partenaire. Une date d'expiration (1 an maximum) est exigée pour ce type de compte.

Les accès de base (compte réseau et espaces de stockage du secteur) seront attribués.

Des validations seront effectuées par la DTI avant l'attribution des droits demandés.

La personne cadre sera sollicitée périodiquement afin qu'elle valide la liste des comptes des partenaires sous sa responsabilité.

6.3.2 Absence et retour au travail

La personne cadre identifiée comme responsable du partenaire doit soumettre une requête à la DTI dès le premier jour d'absence de la personne utilisatrice afin que les accès soient suspendus.

Les accès aux logiciels de gestion seront suspendus dès le premier jour d'absence.

Au retour de la personne utilisatrice, la personne cadre doit soumettre une requête demandant la réactivation des droits d'accès aux logiciels de gestion en fonction des tâches assignées à la ressource. Des validations seront effectuées par la DTI avant l'attribution des droits demandés.

6.3.3 Changement de fonction

La personne cadre identifiée comme responsable du partenaire doit soumettre une requête à la DTI, dès le premier jour du changement de fonction, demandant la modification des droits d'accès aux logiciels de gestion en fonction du nouveau poste de la ressource. Des validations seront effectuées par la DTI avant l'attribution des droits demandés.

La DTI s'assurera de fermer les accès liés aux anciennes fonctions de la personne utilisatrice.

6.3.4 Départ

La personne cadre identifiée comme responsable du partenaire doit soumettre une requête à la DTI dès le départ de la personne utilisatrice afin que les accès soient désactivés.

Le partenaire doit aviser le cadre responsable de tout départ de personnes utilisatrices au sein de son équipe.

La personne utilisatrice ne pourra pas récupérer les données après son départ.

6.3.5 Accès à distance par RPV (VPN)

La personne cadre responsable du partenaire doit soumettre une requête à la DTI pour demander l'accès à distance (RPV) pour la personne utilisatrice. Cet accès est possible uniquement avec un ordinateur appartenant au Cégep.

7. Demande de droits additionnels

La coordination ou la direction responsable de la personne utilisatrice doit soumettre une requête à la DTI demandant les droits d'accès additionnels aux espaces de stockage et aux logiciels de gestion en fonction du poste occupé. Des validations de conformité seront effectuées par la DTI et des autorisations pourraient être demandées aux personnes responsables avant l'attribution des droits.

8. Maintenance et révision de la liste des personnes utilisatrices et de leurs niveaux d'accès

Des révisions régulières de la liste des personnes utilisatrices et de leurs accès seront réalisées tout au long de l'année. La DTI sollicitera les directions, les coordinations et les responsables de logiciels de gestion pour réaliser ces opérations.

9. Maintenance automatisée de la liste des accès

Pour des raisons de sécurité, des opérations régulières de validation de l'utilisation des comptes sont réalisées dans le but de détecter les comptes non utilisés pour les rendre inactifs. Les règles suivantes sont établies :

1. Un nouveau compte n'ayant pas été utilisé 90 jours après sa création sera suspendu.
2. Un compte attribué à un membre du personnel dont le mot de passe doit être modifié depuis plus de 120 jours verra le niveau de sa licence Microsoft diminué à A1. Ce niveau permet seulement l'utilisation du réseau du Cégep, de la boîte courriel, de l'espace de stockage personnel et des outils de base de Microsoft (Word, Excel, PowerPoint).
3. La licence Microsoft d'un membre du personnel absent depuis plus de 90 jours sera abaissée à une licence de type A1.
4. Un compte attribué à un membre du personnel enseignant sera suspendu si le mot de passe réseau n'est pas modifié après plus de 42 mois.
5. Un compte attribué à membre du personnel professionnel, du personnel de soutien ou du personnel cadre dont le mot de passe réseau n'a pas été modifié depuis plus de 30 mois sera suspendu.

Afin de faire réactiver les accès ainsi suspendus, la coordination ou la direction responsable doit, après avoir validé le maintien à l'emploi de la personne, soumettre une requête à la DTI.

10. Accès à distance par RPV (VPN)

Seuls les membres du personnel et les partenaires dûment autorisés utilisant un ordinateur appartenant au Cégep auront l'autorisation d'accéder à distance aux ressources informationnelles du Cégep.

11. Détection de connexion suspecte

Pour des raisons de sécurité, des mécanismes automatisés permanents sont en place pour détecter des tentatives de connexion suspectes aux comptes d'accès.

Ce type de situation peut notamment survenir lorsque des tentatives d'accès soutenues sont faites à partir de plusieurs pays dans un court laps de temps.

Si une utilisation présentant un haut niveau de risque est détectée, le compte sera automatiquement suspendu. Dès lors, la personne utilisatrice sera contactée par la DTI pour l'informer et mettre des mesures de protection en place, si nécessaire. Elle pourrait devoir se présenter rapidement au point de service de la DTI avec son équipement pour rétablir la configuration nécessaire à son bon fonctionnement.

12. Responsable de l'application et de la diffusion

La Direction des technologies de l'information est responsable de l'application de la présente Directive et de sa diffusion auprès des membres du personnel du Cégep.

13. Entrée en vigueur et mise à jour

La présente Directive entre en vigueur au moment de son adoption par le comité de direction, le 18 juin 2025. Elle est mise à jour au besoin.