UQÀM | Université du Québec à Montréal

Directive sur la gestion des identités et des accès

Dernière mise à jour
18 juin 2026

Responsable de l’application	Vice-rectrice, vice-recteur aux Systèmes d’information
Autorité compétente	Vice-rectrice, vice-recteur aux Systèmes d’information
Signature	Louis-Sébastien Guimond Signé avec ConsignO Cloud (25/06/2026) Vérifiez avec verifio.com ou Adobe Reader. UQÀM
Date d’approbation	18 juin 2026
Date d’entrée en vigueur	18 juin 2026
Date de la dernière modification	

Table des matières

1. Objet

La présente directive traite de la gestion des accès aux systèmes d'information de l'Université du Québec à Montréal (ci-après « l'Université ») et des modalités de vérification et de validation de l'identité des personnes qui sont dûment autorisées à accéder à ces systèmes.

La gestion des identités et des accès permet de :

a) protéger les systèmes d'information contre les accès non autorisés;
b) conférer à la personne utilisatrice les droits et privilèges dont elle a besoin dans le cadre de ses fonctions;
c) protéger la personne utilisatrice contre l'usurpation d'identité.

2. Champ d'application

La présente directive concerne tous les systèmes d'information détenus par l'Université et s'applique à toute la communauté universitaire ainsi qu'aux personnes physiques et morales externes détenant un système d'information pour l'Université. Pour plus de clarté, toute personne appelée à utiliser, gérer, exploiter ou traiter les systèmes d'information de l'Université doit respecter la présente directive.

3. Cadre juridique

Cette directive est élaborée en tenant compte notamment du cadre juridique suivant :

a) Politique n^{o} 47 sur la sécurité de l'information.

4. Définitions

Aux fins de la présente directive, les termes suivants se définissent comme suit :

a) authentification : procédure de contrôle consistant à vérifier et à valider l'identité d'une entité qui fait une demande d'accès à un réseau, à un système informatique ou à un logiciel. L'authentification fait généralement suite à l'étape d'identification. Pour une personne, l'authentification consiste le plus souvent à fournir une information qu'elle seule connaît (mot de passe, réponse à une question de sécurité, etc.) ou à utiliser un dispositif qu'elle seule possède (carte à puce, jeton, etc.);

b) authentification multifacteur : authentification qui met en œuvre, de façon concomitante, des procédés de vérification faisant appel à au moins deux facteurs d'authentification différents soit : quelque chose que l'on connaît, quelque chose que l'on possède ou quelque chose que l'on est;

c) identification : opération qui consiste, pour une personne ou pour toute autre entité demandant l'accès au système d'information, à communiquer à ce dernier l'identité dont

elle se réclame. L'identification s'effectue notamment par la saisie d'un code d'utilisatrice, utilisateur; il s'agit soit d'un nom, soit d'un numéro spécifique à l'entité;

d) identité : ensemble des attributs permettant de représenter de manière unique une personne ou toute autre entité dans un système d'information;

e) identité sociale : profil numérique d'une personne utilisatrice, généralement issu d'un fournisseur de services tiers (par ex. Google, Microsoft, Meta, Service gouvernemental d'authentification, etc.), utilisé pour s'authentifier et accéder à un système d'information de l'Université. Cette identité repose sur des informations d'identification gérées par le fournisseur tiers et permet de simplifier la connexion;

f) mot de passe : chaîne de caractères associée à un compte que le titulaire doit entrer lors de la procédure d'accès afin de s'authentifier;

g) personne utilisatrice d'un système d'information : toute personne à qui est accordé l'accès à un système d'information.

5. Identification et authentification

5.1 Identification

L'identification sur les systèmes d'information de l'Université doit se faire par l'entremise d'un identifiant unique et propre à chaque compte utilisateur fourni par les Services informatiques de l'Université.

L'identification peut également se faire par le biais d'identités sociales sur les systèmes supportant ce type d'authentification.

5.2 Authentification

L'authentification aux systèmes d'information de l'Université doit se faire, au minimum, avec un identifiant unique et un mot de passe.

L'authentification à un système d'information doit être intégrée aux infrastructures d'authentification existantes. L'utilisation d'un mécanisme d'authentification différent des infrastructures d'authentification existantes doit être approuvée par la direction de la sécurité de l'information aux Services informatiques.

À l'exception des comptes de service, l'authentification des sessions doit être répétée périodiquement, quelle que soit l'activité de la personne utilisatrice :

a) au moins une fois tous les 5 jours pour un compte utilisateur;
b) au moins une fois tous les 7 jours pour un compte partagé;
c) au moins une fois par jour pour un compte à hauts privilèges.

La session doit être terminée automatiquement lorsque ce délai est atteint.

5.3 Authentification multifacteur

L'authentification multifacteur doit être activée sur tous les systèmes d'information dotés d'un mécanisme de contrôle d'accès, sauf lorsque cela est techniquement impossible ou incompatible avec l'usage prévu. Par ailleurs, tout nouveau système d'information acquis ou développé et comportant un tel mécanisme doit obligatoirement intégrer cette fonctionnalité.

5.4 Changement de mot de passe

Un mot de passe ayant une longueur minimale de 15 caractères et devant comprendre au minimum un chiffre, un symbole, une lettre minuscule et une lettre majuscule n'a pas à être changé périodiquement. Si un mot de passe ne respecte pas ces normes minimales, la direction de la sécurité de l'information détermine la fréquence de changement de mot de passe, qui peut différer d'un système d'information à un autre. Tout mot de passe qui est attribué par défaut à un identifiant unique lors de la création du compte d'accès doit être changé dans un délai de cinq jours suivant la première authentification.

Dans le cas du départ d'une personne utilisatrice ayant eu en sa possession des identifiants et mots de passe de tout autre type de compte d'accès que le compte utilisateur dont elle était propriétaire, le changement des mots de passe associés à ce ou ces comptes doit être fait dans les meilleurs délais.

La personne utilisatrice qui croit que la confidentialité de son mot de passe est compromise a l'obligation de le changer et d'en aviser immédiatement la direction de la sécurité de l'information.

5.5 Confidentialité des mots de passe

La confidentialité des mots de passe doit être préservée par des mécanismes qui assurent, au minimum, que :

a) les mots de passe ne sont pas stockés en clair sur les systèmes d'information;
b) les mots de passe sont transmis par des canaux chiffrés;
c) les outils de gestion et de stockage des mots de passe sont seulement accessibles aux personnes autorisées.

La personne utilisatrice ne doit, en aucun cas, partager le mot de passe des comptes d'accès qu'elle utilise à l'Université.

Dans le but de limiter tout type d'attaque informatique, la direction de la sécurité de l'information peut, à tout moment, désactiver un compte d'accès si elle juge que le mot de passe de ce dernier a été compromis.

6. Types de compte d'accès

6.1 Compte utilisateur

Le compte utilisateur, le plus souvent associé à un identifiant et à un mot de passe, est utilisé par une seule personne utilisatrice et doit être employé pour les tâches courantes.

La personne utilisatrice associée au compte utilisateur en est l'unique propriétaire.

6.2 Compte à hauts privilèges

Le compte à hauts privilèges est attribué à une seule personne utilisatrice qui dispose de privilèges permettant d'administrer les environnements, plateformes et systèmes ou de passer outre les mesures et contrôles mis en place pour des raisons de support. Son utilisation doit être justifiée par la nécessité d'accomplir des tâches d'administration sur le système d'information concerné. La personne utilisatrice associée au compte à hauts privilèges en est l'unique propriétaire. L'utilisation du compte à hauts privilèges doit respecter les critères suivants :

a) la personne utilisatrice ne peut pas utiliser un compte à hauts privilèges pour les opérations habituellement faites avec un compte utilisateur;
b) la personne qui dispose d'un compte à hauts privilèges doit également avoir un compte utilisateur, qu'elle utilise pour les tâches courantes;
c) l'identifiant et le mot de passe d'un compte à hauts privilèges doivent être distincts de ceux du compte utilisateur.

6.3 Compte de service

Le compte de service est attribué à un système ou à une application, habituellement utilisé dans des contextes non-interactifs et s'exécutant sur un serveur pour effectuer automatiquement des tâches planifiées. Il est utilisé pour accomplir des tâches automatisées et des intégrations sur les systèmes d'information, il n'est pas associé à une personne utilisatrice.

6.4 Compte générique

Le compte générique est un compte partagé, donc qui est utilisé par plusieurs personnes utilisatrices dans des cas spécifiques, soient :

a) pour des raisons techniques incontournables qui empêchent l'utilisation d'un compte utilisateur individuel;
b) pour des raisons opérationnelles où l'utilisation d'un système doit être partagée par plusieurs personnes utilisatrices lors de la même session.

7. Gestion des comptes

La personne détentrice d'un compte d'accès est responsable des actions effectuées au moyen de ce compte. Tout compte d'accès de l'Université doit exclusivement être utilisé dans le respect des fonctions et tâches institutionnelles qui lui sont attribuées.

La gestion des comptes d'accès doit se faire en suivant la Norme sur la gestion des comptes d'accès, c'est-à-dire en s'assurant au minimum que :

a) seules les personnes autorisées obtiennent les accès à un compte utilisateur;
b) tout compte d'accès soit associé minimalement à une personne propriétaire;
c) tout compte d'accès soit documenté dans le registre prévu à cet effet;
d) tout compte d'accès soit, au minimum, désactivé lorsque son utilisation n'est plus justifiée.

8. Gestion des droits accès

8.1 Octroi des droits d'accès

L'octroi des droits d'accès doit se faire en suivant la Norme sur la gestion des droits d'accès qui prescrit, au minimum, de :

a) spécifier la raison de la demande d'octroi des droits d'accès;
b) demander l'approbation d'un membre du personnel cadre gestionnaire de l'unité requérante ou de la personne propriétaire du système d'information, selon le cas;
c) valider la conformité des droits d'accès demandés face au rôle et aux fonctions de la personne utilisatrice.

8.2 Révision et modification des droits d'accès

La, le responsable d'un système d'information doit réviser les droits d'accès au système concerné et faire valider cette révision auprès de la direction de la sécurité de l'information.

Cette révision doit être effectuée deux fois par an pour les comptes à hauts privilèges et au moins une fois par an pour les autres comptes, sauf pour les systèmes d'information dont la gestion des comptes est automatisée.

La personne utilisatrice qui se rend compte qu'elle dispose de droits d'accès qui ne sont pas nécessaires pour la réalisation de ses tâches ou de ses fonctions a l'obligation d'en informer la, le responsable du système d'information.

La modification des droits d'accès aux systèmes d'information doit se faire en suivant la Norme sur la gestion des droits d'accès, c'est-à-dire en s'assurant au minimum :

a) d'accorder les droits d'accès nécessaires au rôle et aux responsabilités de la personne utilisatrice dès son entrée en fonction;

b) de révoquer les droits d'accès qui ne sont plus pertinents au nouveau rôle ou aux nouvelles responsabilités de la personne utilisatrice dès son changement de fonction.

8.3 Révocation des droits d'accès

La révocation des droits d'accès aux systèmes d'information doit se faire en suivant la Norme sur la gestion des droits d'accès, laquelle prévoit, au minimum :

a) la désactivation de l'ensemble des comptes d'une personne utilisatrice et des droits d'accès afférents dès la date de fin de son contrat, ou à l'expiration des délais de grâce prévus aux différents contrats de travail de l'Université, le cas échéant;

b) l'interdiction de réattribuer à une nouvelle personne un identifiant unique et des droits d'accès qui étaient auparavant fournis à une autre personne utilisatrice;

c) la description du processus de révocation des droits d'accès en cas de congédiement.

8.4 Accès exceptionnel aux données d'un compte utilisateur

De façon exceptionnelle et lorsque requis pour assurer la continuité des activités, une personne qui exerce le rôle de gestionnaire à l'Université peut faire une demande d'accès aux données d'une personne utilisatrice dont elle est responsable.

Cette demande d'accès exceptionnel doit se faire en suivant la Norme sur l'octroi ou la modification des droits d'accès aux données d'une autre personne utilisatrice. En outre, le processus ne peut être entamé qu'après avoir obtenu l'autorisation de la vice-rectrice, du vice-recteur à la Vie académique dans le cas des personnes enseignantes et étudiantes, de la vice-rectrice, du vice-recteur au Développement humain et organisationnel dans le cas des personnes non-enseignantes, et de la vice-rectrice, du vice-recteur aux Systèmes d'information, ou, en cas d'absence desdites vice-rectrices, desdits vice-recteurs concernés, de la rectrice, du recteur.

La personne à qui appartient le compte utilisateur dont les données ont été ainsi partagées, ou son ayant-droit dans le cas d'une personne décédée, doit être informée des accès autorisés, du motif de leur autorisation et de la durée des accès. Dans tous les cas, l'accès aux données d'une personne utilisatrice doit être accordé en conformité avec les lois applicables.

9. Responsable de l'application

La vice-rectrice, le vice-recteur aux Systèmes d'information est responsable de l'application de cette directive.

10. Entrée en vigueur

La présente directive entre en vigueur dès son adoption par la vice-rectrice, le vice-recteur aux Systèmes d'information.

11. Mise à jour

Cette directive est mise à jour minimalement tous les cinq ans.