UQAR Université du Québec à Rimouski

TITRE : **DIRECTIVE RELATIVE À LA GESTION DES IDENTITÉS ET DES ACCÈS AUX ACTIFS INFORMATIONNELS SUR UN SUPPORT NUMÉRIQUE**

APPROUVÉE PAR: COMITÉ EXÉCUTIF

CODE : **C3-D119**

EN VIGUEUR : 19-05-2026

RÉS. : EX-911-7148
19-05-2026

RESPONSABILITÉ : SERVICE DES TECHNOLOGIES DE L'INFORMATION

RÉVISION PRÉVUE : 2031

TABLE DES MATIÈRES

1 PRÉAMBULE

1.1 La présente directive s'inscrit dans la foulée de la modernisation de l'encadrement applicable à la protection des renseignements personnels et à la sécurité de l'information des organismes publics. Ces règles requièrent que les organismes publics exercent un contrôle sur les accès aux actifs informationnels et à l'information qui y est détenue.

1.2 Elle découle du *Cadre de gestion de la sécurité de l'information* et de la *Politique sur la gestion et sur le contrôle des accès aux actifs informationnels* de l'Université, compte tenu des innombrables avancées technologiques, des incidents de cybersécurité et des fuites de renseignements personnels qui compromettent la vie privée des personnes citoyennes du Québec.

2 OBJECTIFS

2.1 La présente directive a pour objectif de mettre en œuvre le cadre général prévu à la *Politique sur la gestion et sur le contrôle des accès aux actifs informationnels* de l'Université et de l'appliquer spécifiquement aux actifs informationnels sur support numérique.

2.2 Elle a donc pour objectif d'établir les principes directeurs, rôles et responsabilités relatifs à la gestion des identités et des accès aux actifs informationnels sur support numérique en vue de protéger l'information que l'Université détient sur ceux-ci.

3 CADRE JURIDIQUE

La présente directive est élaborée en tenant compte du cadre juridique suivant :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ c. G-1.03);
- Programme de sensibilisation à la sécurité de l'information;
- C3-D30 *Directive relative à l'utilisation et à la gestion des technologies de l'information et des télécommunications*;
- C3-D99 *Politique de la sécurité de l'information*;
- C3-D109 *Cadre de gestion de la sécurité de l'information*;
- C3-D110 *Procédure relative à la gestion des incidents de confidentialité impliquant des renseignements personnels*;
- C3-D118 *Politique sur la gestion et sur le contrôle des accès aux actifs informationnels;*
- *C3-D97 Politique de gestion des risques*.

4 CHAMP D'APPLICATION

4.1 La présente directive s'adresse principalement aux personnes membres de la communauté universitaire qui ont comme responsabilité la gestion des identités et des accès aux actifs informationnels sur support numérique de l'Université.

4.2 La présente directive s'adresse également aux membres de la communauté universitaire qui ont ou sont susceptibles d'avoir accès aux actifs informationnels sur support numérique de l'Université dans le cadre de leurs fonctions ou de leur mandat, c'est-à-dire, sans s'y limiter, le personnel cadre, les professeures et professeurs, les personnes chargées de cours, le personnel administratif et de soutien, les personnes étudiantes de même que toute personne physique ou morale qui agit à titre de personne consultante, de partenaire ou à titre de fournisseur de services.

5 DÉFINITIONS

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

Actif informationnel : tout système d'information, réseau de télécommunication, infrastructure ou un ensemble de ces éléments contenant de l'information. Un actif informationnel peut être sur un support numérique (système d'information, réseau, etc.) ou sur un support physique (local, bureau, classeur, salle des serveurs, etc.).

Actif informationnel sur un support numérique : tout système d'information, réseau de télécommunication, infrastructure technologique ou un ensemble de ces éléments contenant un document ou de l'information sur un support numérique.

Accès, ou droit d'accès : droit accordé à une personne utilisatrice lui permettant d'accéder à un actif informationnel.

Accès à haut privilège : accès particulier offrant des capacités supérieures à un niveau d'accès régulier ou permettant d'accéder à de l'information sensible.

Authentification : processus qui consiste à valider l'identité d'une personne utilisatrice ou d'un système. Ce processus intervient directement après le processus d'identification. Une personne utilisatrice utilise un ou des authentifiants (Ex.: mot de passe, code secret, application d'authentification, etc.) qu'elle seule connait ou possède.

Authentification multifactorielle (MFA) : procédé de vérification faisant appel à au moins deux (2) facteurs d'authentification différents.

Autorisation : processus qui consiste à accorder des accès à une personne utilisatrice.

Communauté universitaire : désigne toute personne, qui notamment :

- exerce une fonction, occupe un emploi rémunéré ou accomplit des tâches bénévolement à l'Université;
- poursuit des études à l'Université;
- poursuit des activités à titre de stagiaire (incluant un stage postdoctoral);
- fait partie d'une association ou d'un groupe relié à l'Université;
- a des relations avec l'Université à titre de personne cliente, visiteuse, invitée, ayant des contrats de services ou d'approvisionnement avec l'Université, sous-traitante ou locataire.

Identification : processus qui consiste à établir l'identité d'une personne utilisatrice. Une personne utilisatrice utilise un identifiant (Ex.: « Identifiant UQAR », code utilisateur, etc.) unique qui lui est attribué individuellement.

Identifiant générique : identifiant qui n'est pas exclusif à une seule personne utilisatrice.

Identifiant UQAR : identifiant unique attribué à une personne utilisatrice des systèmes d'information, réseau de télécommunication, infrastructure technologique de l'Université. Il est composé d'une chaine de caractères alphanumériques se terminant par « uqar.ca ».

Information : élément, détail, fait, renseignement, ou donnée sur quelque chose ou quelqu'un. L'information est contenue sur un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments et constitue un actif informationnel.

Information sensible : information qui, par sa nature ou en raison de son contexte, suscite un haut degré d'attente raisonnable en matière de confidentialité.

Journalisation : enregistrement chronologique, dans un fichier ou une base de données, des opérations effectuées dans un système informatique ou un programme.

Personne utilisatrice : toute personne membre de la communauté universitaire qui utilise un actif informationnel de l'Université ou qui y a accès.

Personne utilisatrice externe : personne utilisatrice n'ayant pas de lien d'emploi ou d'étude avec l'établissement.

Principe de nécessité : principe fondamental ayant pour objectif de réduire les atteintes à la vie privée des personnes concernées par les renseignements personnels détenus par l'Université et les risques en matière de sécurité de l'information. Il doit prédominer en toute circonstance.

Principe de séparation des tâches : principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible sont réparties entre plusieurs entités (personnes, processus, etc.) afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité.

Principe du droit d'accès minimal : principe selon lequel il convient d'accorder à la personne utilisatrice uniquement les autorisations d'accès dont elle a besoin pour accomplir ses tâches.

Système d'information : ensemble organisé de moyens mis en place pour recueillir, stocker, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un objectif ou besoin déterminé, incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions. Un fichier ou document individualisé n'est pas un système d'information en soi.

Il peut s'agir entre autres d'une ou d'un :

- système informatique de traitement des dossiers;
- logiciel de vidéoconférence ou de collaboration;
- système biométrique;
- système d'intelligence artificielle (IA);
- système de cartes à puce/RFID;
- système de vidéosurveillance;
- système statistique;
- système de gestion de la paie;
- dossier électronique;
- application mobile;
- site Web.

6 RÔLES ET RESPONSABILITÉS

6.1 Personne cheffe de la sécurité de l'information organisationnelle (CSIO)

La personne CSIO est responsable de superviser la mise en œuvre et le suivi de la gestion des identités et des accès à l'Université, notamment, elle :

a) s'assure du respect des obligations en matière de gestion des identités et des accès (GIA);
b) s'assure de l'application et de la mise à jour de la présente directive;
c) détermine les modalités de vérification de l'identité;
d) s'assure de l'existence d'activités de formation et de sensibilisation en matière de GIA offertes aux personnes utilisatrices;

e) approuve les demandes de dérogation formulées en application de la présente directive;
f) veille à la mise en œuvre et au suivi des processus de révision des accès, notamment que ceux-ci soient lancés et suivis régulièrement.

6.2 Personne détentrice de l'information

Pour l'information sous leur responsabilité, la personne détentrice :

a) est imputable des actions pouvant découler des accès accordés;
b) s'assure de l'application de la présente directive;
c) s'assure de la mise en œuvre de processus et règles d'affaires en matière de GIA;
d) s'assure de l'approbation des demandes d'attribution, de révision ou de retrait d'accès qui lui sont soumises;
e) maintient le registre des accès à haut privilège attribués.

6.3 Secrétariat général

Dans le cadre de cette directive, le Secrétariat général :

a) contribue à l'élaboration et à la révision de la présente directive;
b) appuie la personne CSIO en matière de GIA;
c) appuie les personnes détentrices de l'information ou les personnes les représentant dans la mise en place des processus et règles d'affaires en matière de GIA;

6.4 Service des technologies de l'information

Dans le cadre de cette directive, le Service des technologies de l'information :

a) est responsable de l'application et de la révision de la présente directive;
b) appuie la personne CSIO en matière de GIA;
c) appuie les personnes détentrices de l'information ou les personnes les représentant dans la mise en place des processus et règles d'affaires en matière de GIA;
d) définit et met en place les mesures et mécanismes de protection nécessaires à la mise en œuvre de la présente directive notamment :
   - est responsable de créer, modifier et supprimer les comptes utilisateurs, plus précisément :
     - exécute les opérations d'attribution, de révision ou de retrait des accès pour les actifs informationnels qu'il administre, après approbation de la personne détentrice de l'information;
     - exécute les processus d'épuration des comptes conformément aux règles définies en collaboration avec les personnes détentrices de l'information;
   - détermine les règles en matière de gestion des mots de passe, notamment :
     - la fréquence des changements;
     - les critères de complexité;
     - la réutilisation des mots de passe utilisés antérieurement;
   - établit les bonnes pratiques et recommandations quant à l'utilisation d'un gestionnaire de mot de passe;
e) analyse les journaux et historiques d'accès pour détecter des irrégularités concernant la GIA;
f) met à jour le registre des identités et accès.

6.5 Personne utilisatrice

La personne utilisatrice doit prendre les mesures nécessaires afin d'utiliser responsablement ses accès et préserver la confidentialité de ses informations d'identification, notamment, elle :

a) évite de contourner les processus d'identification et d'authentification;
b) n'utilise pas les informations d'identification de l'Université de façon malveillante, notamment par l'usurpation de l'identité d'une autre personne;
c) stocke ses mots de passe de manière adéquate;
d) évite de transmettre les informations relatives à ses identifiants et de partager ses accès avec une personne tierce;
e) est responsable des activités résultant de l'usage de son identifiant et des autorisations qui lui sont attribuées;
f) évite d'utiliser des informations d'identification de l'Université (identifiant UQAR ou courriel) pour un service/système externe en dehors du cadre de ses fonctions ou de ses études. De même, lorsqu'une situation exceptionnelle nécessite que des informations d'identification de l'Université soient utilisées pour un service/système externe, la personne utilisatrice doit choisir un mot de passe différent de celui utilisé à l'Université;
g) signale toute irrégularité, tout évènement ou incident susceptible d'avoir des impacts sur ses accès auprès de la personne détentrice de l'information ou du Service des technologies de l'information.

6.6 Personnel cadre

Le personnel cadre, en collaboration avec les personnes détentrices de l'information, est responsable de :

a) gérer les demandes d'accès pour les personnes sous leur responsabilité;
b) valider les besoins d'accès selon les rôles et responsabilités de chaque personne sous leur responsabilité;
c) s'assurer que les accès correspondent aux besoins opérationnels;
d) signaler à la personne détentrice de l'information ou au Service des technologies de l'information tout changement de statut concernant les personnes titulaires d'un accès sous leur responsabilité.

7 PRINCIPES DIRECTEURS ET RÈGLES D'AFFAIRES

La gestion des identités et accès à l'Université repose sur des principes directeurs et des règles d'affaires spécifiques à certains types d'accès qui seront définis par le Service des technologies de l'information.

7.1 Principes généraux

L'accès à un actif informationnel se fonde sur le principe de nécessité et sur le principe du droit d'accès minimal.

7.2 Accès

a) L'accès à un actif informationnel sur un support numérique doit inclure une procédure de connexion sécurisée et prendre en compte l'identification, l'authentification et l'autorisation.

b) L'accès à un actif informationnel exposé à l'internet doit employer une authentification multifactorielle.

c) Un accès attribué à une personne utilisatrice externe est soumis à des règles particulières déterminées, notamment :

- une limitation de la durée de l'attribution;
- la nécessité d'être parrainé par un membre du personnel autorisé;
- le respect des critères de sécurité appropriés.

7.3 Identifiant

a) Un identifiant générique ou partagé est généralement proscrit. Lorsqu'un identifiant générique est nécessaire, son utilisation doit être documentée et approuvée par le Service des technologies de l'information et il sera nécessaire d'utiliser des contrôles compensatoires pour assurer la sécurité de l'identifiant.

b) Les processus d'attributions et d'épurations des identifiants UQAR sont formellement définis et documentés. Ils prévoient notamment l'attribution d'un identifiant UQAR à une personne utilisatrice tant qu'un lien officiel avec l'Université est existant, notamment :

- une affectation d'emploi active;
- un statut d'admission à un programme d'études ou l'inscription à un programme d'études, selon les règles d'affaires en vigueur;
- selon les règles ou conventions particulières.

c) Les accès qui sont rattachés à un identifiant sont destinés à l'usage exclusif de la personne utilisatrice à qui ils sont attribués.

d) Lorsque le lien entre une personne et l'Université est rompu, l'identifiant rattaché à cette personne est révoqué et ne peut être réutilisé.

7.4 Octroi, révision et retrait des accès

a) Les processus d'octroi des accès se fondent sur le principe de séparation des tâches.

b) Les processus d'octroi, de révision et de retrait des accès sont formellement définis et documentés. Ils prévoient notamment :

- la révision des accès à hauts privilèges deux (2) fois par année;
- la révision de l'ensemble des accès une (1) fois par année.

c) Le départ, le transfert, la mutation ou tout autre changement de statut d'une personne utilisatrice conduit systématiquement à la révision de ses d'accès et au retrait de ceux qui ne respectent plus les règles d'octroi.

7.5 Mécanismes de contrôle et de protection

a) Un actif informationnel sur un support numérique de l'Université doit être protégé adéquatement contre tout accès non autorisé et contre toute perte ou tout dommage qui pourrait être causé de façon accidentelle ou délibérée.

b) Les mécanismes de contrôle des accès doivent être proportionnels au niveau de criticité d'un actif informationnel et de sensibilité des accès attribués, notamment un accès peut être soumis à des mesures telles que :

- la journalisation des connexions et des actions;
- une limitation de la durée de l'attribution de l'accès;
- une limitation du champ d'action possible, etc.

c) Des mécanismes de protection des mots de passe sont formellement documentés et définis afin d'en assurer la protection, ils prévoient notamment que :

- tous les mots de passe doivent respecter les règles établies par le Service des technologies de l'information en matière de gestion des mots de passe;
- tous les mots de passe par défaut fournis par un fournisseur doivent être modifiés afin de respecter les règles établies avant qu'un système puisse être installé sur le réseau;

- si la sécurité d'un mot de passe est mise en doute, le mot de passe doit être changé immédiatement;
- un mot de passe doit être chiffré et entreposé sur un support informatique sécurisé (fichier, base de données, stockage d'entreprise, etc.);
- un système de gestion de mots de passe est utilisé en conformité avec les recommandations fournies par le Service des technologies de l'information;
- lorsqu'une situation exceptionnelle nécessite qu'un mot de passe soit conservé sur un support non informatique, il doit être conservé sous clé.

8 DÉROGATIONS

8.1 La présente directive constitue la règle générale applicable à l'ensemble de la communauté universitaire. Toutefois, des situations exceptionnelles peuvent justifier l'octroi de dérogations, lorsqu'il n'existe aucune autre alternative raisonnable pour permettre la continuité des activités académiques, administratives ou de recherche.

8.2 Toute demande doit être écrite, justifiée et soumise à la direction du Service des technologies de l'information qui, au besoin, sollicitera le CSIO pour approbation. Les dérogations doivent être temporaires, examinées régulièrement et retirées dès qu'elles ne sont plus nécessaires.

9 REGISTRE DES ACCÈS

L'Université doit tenir à jour un registre des identités et des accès.

10 RESPONSABLE DE L'APPLICATION

Le Service des technologies de l'information est responsable de l'application de cette directive.

11 MISE À JOUR

La présente directive est mise à jour tous les cinq (5) ans, ou plus souvent si des modifications sont nécessaires.

12 ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à la date de son adoption par le Comité exécutif.