UQAR Université du Québec à Rimouski

TITRE :	**POLITIQUE SUR LA GESTION ET SUR LE CONTRÔLE DES ACCÈS AUX ACTIFS INFORMATIONNELS**		
APPROUVÉE PAR:	CONSEIL D'ADMINISTRATION	CODE :	**C3-D118**
EN VIGUEUR :	19-05-2026	RÉS. :	CA-814-9875 19-05-2026
RESPONSABILITÉ :	SECRÉTARIAT GÉNÉRAL		
RÉVISION PRÉVUE :	2031		

TABLE DES MATIÈRES

1 PRÉAMBULE

La présente politique 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 octroyés à leurs actifs informationnels et à l'information qui y est détenue.

2 OBJECTIFS

2.1 La présente politique a pour objectifs de prévoir les principes généraux applicables à la gestion et au contrôle des accès aux actifs informationnels de l'Université, en vue de protéger l'information qu'elle détient.

2.2 Elle précise les règles applicables à la gestion et au contrôle des accès aux actifs informationnels octroyés aux membres de la communauté universitaire, que ces actifs soient sur un support physique ou numérique.

2.3 Les règles générales édictées par la présente politique serviront de cadre de référence pour les membres de la communauté universitaire pour l'utilisation de leurs accès ainsi qu'aux responsables de l'octroi des accès dans l'élaboration de leurs processus de gestion et de contrôle des accès respectifs.

3 CADRE JURIDIQUE

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

- la *Loi sur l'Université du Québec* (RLRQ, ch. U-1);
- la *Charte des droits et libertés de la personne* (RLRQ, ch. C-12);
- le *Code civil du Québec* (RLRQ, ch. CCQ-1991);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, ch. G-1.03);
- la *Loi concernant le cadre juridique des technologies et l'information* (RLRQ, chapitre C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- la *Loi sur les renseignements de santé et de services sociaux*;
- la *Loi sur les archives* (RLRQ, chapitre A-21.1);
- la *Loi canadienne sur les droits de la personne* (LRC, 1985, chapitre H-6);
- le *Code criminel* (LRC, 1985, chapitre C-46);
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r. 02);
- la *Directive sur la sécurité de l'information gouvernementale*;
- Règlement 15 : *Registres officiels et documentation administrative de l'Université*;
- C3-D99 *Politique sur la sécurité de l'information*;
- C3-D109 *Cadre de gestion de la sécurité de l'information*;
- C3-D111 *Politique établissant le cadre de gouvernance en matière de protection des renseignements personnels*;
- C3-D112 *Directive sur la collecte, l'utilisation et la communication de renseignements personnels*;

- C3-D119 *Directive relative à la gestion des identités et des accès aux actifs informationnels sur support numérique*.

4 CHAMP D'APPLICATION

4.1 La présente politique s'adresse principalement aux membres de la communauté universitaire qui ont comme responsabilité la gestion et le contrôle des accès aux actifs informationnels de l'Université.

4.2 Elle s'adresse également aux membres de la communauté universitaire qui ont ou sont susceptibles d'avoir accès aux actifs informationnels de l'Université dans le cadre de leurs fonctions ou 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 politique, 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.).

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

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.

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.

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

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.

Renseignement personnel : désigne un renseignement ou un regroupement de renseignements qui porte sur une personne physique et permet de l'identifier. Un renseignement personnel est confidentiel. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement concernant cette personne ou lorsque sa seule mention révèlerait un renseignement personnel la concernant.

Sont notamment du domaine public et ne sont pas personnels les renseignements suivants :

- nom, titre, fonction, classification, traitement, l'adresse et le numéro de téléphone professionnels d'un membre du personnel d'un organisme public;
- un renseignement concernant une personne en sa qualité de partie à un contrat de service conclu avec un organisme public.

Renseignement personnel sensible : désigne un renseignement personnel qui, notamment par sa nature médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de respect de la vie privée.

Support : moyen de conservation et de diffusion d'information autre qu'un système d'information. Un support peut être numérique (clé USB, carte mémoire, appareil mobile, bande de copie, disque externe, vidéo, etc.) ou papier.

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 RESPONSABILITÉ

6.1 Personne cheffe de la sécurité de l'information organisationnelle (CSIO) et responsable de la protection des renseignements personnels

La secrétaire générale ou le secrétaire général est la personne désignée comme personne cheffe de la sécurité de l'information organisationnelle et responsable de la protection des renseignements personnels pour l'Université. Elle s'assure que les accès aux actifs informationnels

de l'Université soient octroyés, révisés et retirés conformément au cadre juridique et normatif applicable.

6.2 Personne responsable de l'octroi d'un accès

La personne responsable de l'octroi d'un accès à un actif informationnel de l'Université doit s'assurer que celui-ci respecte les principes généraux énumérés à la présente politique ainsi que ceux spécifiques à un type d'actif informationnel énumérés dans les directives ou procédures appropriées.

6.3 Personne utilisatrice

Toute personne ayant reçu un accès à un actif informationnel de l'Université doit s'assurer de mettre en œuvre toutes les mesures adéquates afin d'assurer la sécurité de l'information et la protection des renseignements personnels. Cette personne doit, notamment :

a) respecter les modalités d'octroi de ses accès;
b) protéger, en tout temps, la confidentialité de l'information à laquelle elle a accès;
c) ne pas partager ses accès avec une personne tierce;
d) déclarer tout changement à ses fonctions ou à son mandat susceptible d'avoir un impact sur les accès qui lui sont octroyés.

7 PRINCIPES GÉNÉRAUX

7.1 Les accès aux actifs informationnels de l'Université doivent être contrôlés de manière à protéger adéquatement l'information qui y est détenue en fonction de sa sensibilité, de son utilité et au degré de confidentialité requis.

7.2 Ainsi, seules les personnes détenant les autorisations requises peuvent accéder à l'information détenue par l'Université. Les accès doivent être révisés périodiquement en fonction de la sensibilité de l'information détenue, des mouvements de personnel et des besoins de l'Université.

8 GESTION ET CONTRÔLE DES ACCÈS

8.1 Principes de nécessité, d'accès minimal et de séparation des tâches

a) Tout octroi, révision ou retrait d'accès doit respecter les principes de nécessité, d'accès minimal et de séparation des tâches.

b) Dans le contexte de la présente politique, ces principes seront respectés si les niveaux d'accès sont justifiés, lorsque la personne concernée n'aura accès qu'à l'information nécessaire à l'exercice de ses fonctions ou à l'exécution du mandat qui lui a été octroyé et que la sensibilité de l'information aura été prise en compte.

8.2 Octroi des accès

a) Avant d'octroyer l'accès à un actif informationnel, la personne responsable de cet octroi doit s'assurer que la personne utilisatrice y est autorisée et que ses fonctions ou son mandat justifient l'accès. Dans le cas où l'information accessible n'est pas nécessaire aux fonctions ou au mandat de la personne qui le requiert, l'accès doit être refusé.

b) Si l'information accessible contient des renseignements personnels ou autrement confidentiels, la personne responsable de l'octroi doit également s'assurer que:

- l'entente ou le consentement rattaché à la collecte des renseignements concernés permet cet accès;

- la personne qui requiert l'accès a signé les engagements de confidentialité requis avant d'accéder aux renseignements.

c) Les accès octroyés doivent être individualisés, c'est-à-dire qu'ils sont rattachés à une personne seulement.

8.3 Accès externes

a) Si la personne qui requiert l'accès à un actif informationnel pour la réalisation d'un mandat ou l'exécution d'un contrat de service n'est pas une personne étudiante ou une personne membre du personnel de l'Université, l'octroi de celui-ci doit respecter les modalités prévues à 8.2 et doit être limité dans le temps. Un tel accès doit donc prendre fin à la première des éventualités suivantes:

- à la date où la personne n'a plus besoin d'accéder à l'actif informationnel visé pour poursuivre l'exécution de son mandat ou la réalisation de son contrat de service;
- à la date où le mandat ou le contrat de service prend fin.

b) Pour tout octroi d'accès externes, la personne ou l'organisme externe est imputable de la saine gestion de ces accès et devra remplir les engagements requis pour l'octroi de ceux-ci.

c) Nonobstant le dernier paragraphe de l'article 8.2, les accès octroyés à une personne externe peuvent être rattachés à un groupe de personnes effectuant les mêmes fonctions s'il est démontré que l'individualisation n'est pas raisonnable, selon le contexte du mandat ou contrat de service.

8.4 Révision et retrait des accès

a) Tout accès octroyé dans le cadre de la présente politique doit être retiré lorsque les principes généraux et les modalités spécifiques aux différents types d'actifs informationnels ne sont plus rencontrés.

b) Les accès aux actifs informationnels de l'Université doivent être révisés périodiquement. La périodicité de la révision des accès doit être établie par les services concernés en fonction de la nature de l'information détenue, notamment de sa sensibilité et de son volume.

9 MANQUEMENTS

9.1 Tout évènement pouvant compromettre l'intégrité des accès aux actifs informationnels constitue un incident de sécurité devant être déclaré sans délai selon les directives en vigueur.

9.2 Le non-respect des termes de la politique par une personne utilisatrice peut entrainer la suspension de ses accès et peut également mener à l'imposition de mesures disciplinaires.

10 RESPONSABLE DE L'APPLICATION

Le secrétariat général est responsable de l'application de cette politique.

11 MISE À JOUR

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

12 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le Conseil d'administration.