

Règlement sur l'utilisation responsable des technologies de l'information

Approbation :	Conseil d'administration (Résolution CA-2022-186)
Entrée en vigueur :	27 octobre 2022
Responsable : et révision	Vice-rectorat aux infrastructures et à la transformation
Cadre juridique :	<i>Charte des droits et libertés de la personne, L.R.Q., c. C-12</i> <i>Code civil du Québec, L.Q. 1991, c-64</i> <i>Code criminel, L.R. 1985, ch. C-46</i> <i>Loi sur le droit d'auteur, L.R. 1985, ch. C-42</i> <i>Loi sur la protection des renseignements personnels et les documents électroniques, L.R. 2000, ch. 5</i> <i>Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1)</i> <i>Loi sur les archives (L.R.Q. c. A-21.1)</i> <i>Loi sur la gouvernance des ressources informationnelles des organismes publics et des entreprises du gouvernement</i>



TABLE DES MATIÈRES

Préambule.....	3
1. Définitions	3
2. Objectifs.....	3
3. Champs d'application	4
4. Obligations générales.....	4
4.1 Identifiant et authentifiant.....	4
4.2 Accès et utilisation des technologies de l'information	5
4.3 Comportement numérique responsable	6
5. Mesures exceptionnelles.....	6
6. Vérification des technologies de l'information	6
7. Signalement et dénonciation.....	6
8. Sanctions	7
9. Dérogation	7
10. Révision du règlement	7
11. Adoption et date d'entrée en vigueur	7

PRÉAMBULE

Les technologies de l'information de l'Université Laval sont mises à la disposition des membres pour la réalisation d'activités d'enseignement, d'apprentissage, de recherche, de gestion et d'administration ainsi que pour les services à la collectivité reliés à la réalisation de la mission de l'Université. Une utilisation responsable des technologies de l'information de l'Université doit se faire de manière sécuritaire, éthique et dans le respect de la vie privée des personnes. Il est important de rappeler que la sécurité et la préservation de l'information sont une responsabilité partagée par chaque membre de l'Université Laval.

L'utilisation et l'accès aux technologies de l'information de l'Université constituent un privilège et non un droit. Seuls les membres autorisés peuvent utiliser et avoir accès aux technologies de l'information de l'Université dans les limites de l'autorisation accordée. La capacité d'accéder aux technologies de l'information de l'Université et de les utiliser ne constitue pas une autorisation de le faire.

Les membres autorisés doivent utiliser les technologies de l'information de l'Université aux fins indiquées d'une manière responsable, éthique et licite, conformément aux politiques, aux directives et aux procédures de l'Université et à d'autres normes et lignes directrices pertinentes de l'Université, et dans le respect des lois et des règlements applicables ainsi que, dans certaines circonstances, des contrats et des ententes de l'Université.

Les membres peuvent raisonnablement s'attendre à ce que leur vie privée soit respectée lorsqu'ils utilisent les technologies de l'information de l'Université.

1. DÉFINITIONS

Membre

Les étudiantes, les étudiants, le corps professoral, le personnel enseignant, le personnel de recherche, les administrateurs, les administratrices et le personnel administratif.

Officière ou officier de la sécurité de l'information

Personne nommée par l'Université aux fins d'établir et faire respecter les orientations et règles de sécurité de l'information. Cette personne relève de la Direction des technologies de l'information.

Technologies de l'information

Ensemble d'outils et de ressources technologiques servant à la collecte, l'utilisation, le traitement, la communication et la conservation de l'information, notamment les ordinateurs, les réseaux dont le sans-fil, les logiciels, les technologies et appareils de diffusion en direct et en différé, les sites Internet, et la téléphonie.

2. OBJECTIFS

Le présent règlement encadre l'utilisation responsable des technologies de l'information de l'Université. Il fixe les règles et conditions applicables à leur utilisation ainsi que les limites et les responsabilités qui en découlent.

Les objectifs du présent règlement sont de :

- Définir les droits et les obligations des membres au regard de l'utilisation des technologies de l'information de l'Université;
- S'assurer de l'utilisation sécuritaire, légale et éthique des technologies de l'information de l'Université;
- S'assurer de la protection des informations détenues par l'Université.

3. CHAMPS D'APPLICATION

Le présent règlement s'applique aux membres de la communauté universitaire qui utilisent des technologies de l'information de l'Université.

L'Université s'attend à ce que les règles et les normes de comportement et d'usage éthique prévues dans le présent règlement soient respectées par les membres de l'Université, et ce même lors de l'emploi d'équipement personnel, si ceux-ci sont mis en lien avec des technologies de l'information de l'Université.

4. OBLIGATIONS GÉNÉRALES

4.1 Identifiant et authentifiant

- 4.1.1 Les membres doivent fournir des données d'identification et d'authentification valides et complètes lorsque requis par l'Université pour l'utilisation des technologies de l'information.
- 4.1.2 Les membres doivent rectifier leurs données d'identification et d'authentification en cas d'inexactitude ou de changement.
- 4.1.3 Lors du processus de demande d'accès aux technologies de l'information, les membres doivent se soumettre aux étapes de vérification d'identité nécessaires en vue de l'émission de :
- Ses identifiants;
 - Ses mots de passe;
 - Ses questions et réponses secrètes si applicable;
 - Tout autre moyen requis pour accéder aux technologies de l'information dont elle ou il a l'autorisation d'usage à l'Université.
- 4.1.4 Les membres, possédant une autorisation d'usage, doivent s'identifier et s'authentifier (lorsque demandé) pour accéder aux technologies de l'information de l'Université.
- 4.1.5 Les membres sont responsables des activités résultant de l'usage de leurs identifiants et des mots de passe liés à ceux-ci.
- 4.1.6 Les membres ne doivent pas partager ou divulguer :
- leurs mots de passe;
 - leurs questions et réponses secrètes si applicable;
 - tout autre moyen rendu disponible pour accéder aux technologies de l'information de l'Université Laval.
- 4.1.7 Les membres doivent, dans les meilleurs délais, modifier un mot de passe, si elle ou il juge que la confidentialité du mot de passe est ou pourrait avoir été compromise, et en aviser dans les meilleurs délais l'Officière ou l'Officier de la sécurité de l'information.
- 4.1.8 Les membres doivent, dans les meilleurs délais, modifier leurs mots de passe si l'Officière ou l'Officier de la sécurité de l'information en fait la demande.
- 4.1.9 Les membres doivent signaler tout usage non autorisé, frauduleux ou abusif d'un identifiant, d'un mot de passe, de ses questions et réponses secrètes ou de tout autre moyen utilisé pour accéder aux technologies de l'information de l'Université.

4.2 Accès et utilisation des technologies de l'information

- 4.2.1 Les membres doivent utiliser les technologies de l'information mises à leur disposition par l'Université uniquement aux fins pour lesquelles elles sont prévues.
- 4.2.2 Les membres doivent assurer la sécurité des équipements personnels mis en lien avec les technologies de l'information de l'Université. Les membres doivent respecter les directives en appliquant les normes institutionnelles établies en matière de sécurité de l'information pour ces équipements personnels.
- 4.2.3 Les membres doivent agir de façon à ne pas nuire à l'accessibilité et à la performance des technologies de l'information de l'Université.
- 4.2.4 Les membres doivent agir de façon à ne pas altérer l'intégrité des technologies de l'information de l'Université ou des informations qui y sont conservées.
- 4.2.5 Les membres doivent restreindre leurs actions sur les technologies de l'information de l'Université à celles qui n'engendrent pas de frais supplémentaires, à moins d'y être spécifiquement et préalablement autorisé par écrit.
- 4.2.6 Les membres doivent respecter le critère de confidentialité des informations auxquelles elles ou ils ont accès.
- 4.2.7 Les membres doivent signaler toute situation susceptible d'affecter la sécurité des technologies de l'information dont il est victime ou témoin. Notamment :
- Le corps professoral, le personnel enseignant, le personnel de recherche, les administrateurs, les administratrices et le personnel administratif doivent signaler à leur gestionnaire tout équipement technologique contenant des informations confidentielles de l'Université ou des renseignements personnels qui serait perdus, égarés ou qui semble être disparus;
 - Les membres doivent rapporter au Service de sécurité et de prévention tout équipement technologique de l'Université Laval qu'elle ou il aurait trouvé.
- 4.2.8 Les membres doivent collaborer, lorsque cela est nécessaire, avec l'Officière ou l'Officier de la sécurité de l'information concernant toute situation susceptible d'affecter la sécurité des technologies de l'information.
- 4.2.9 Les membres ne doivent pas contourner ou essayer de contourner les dispositifs de sécurité des technologies de l'information de l'Université.
- 4.2.10 Les membres ne doivent pas chercher à intercepter, collecter, prendre connaissance, décrypter ou décoder des informations qui ne leur sont pas destinées.
- 4.2.11 Les membres ne doivent pas effectuer des détections de vulnérabilités, des tests d'intrusion ou de la reconnaissance des technologies de l'information de l'Université, à moins que ce soit prévu dans leurs fonctions ou qu'une autorisation écrite ait été obtenue.
- 4.2.12 Les membres ne doivent pas copier, enregistrer, télécharger ou reproduire des informations confidentielles de l'Université ou contenant des renseignements personnels sur des équipements personnels.
- 4.2.13 Les membres ne doivent pas utiliser, télécharger, installer, distribuer ou partager des programmes ou des logiciels sur les technologies de l'information de l'Université, à moins que ce soit prévu dans leurs fonctions ou qu'une autorisation écrite ait été obtenue.

4.2.14 Les membres ne doivent pas utiliser les technologies de l'information de l'Université pour réaliser notamment les actions suivantes:

- participer à une chaîne de lettres;
- effectuer de la publicité à des fins non autorisées;
- participer à des activités commerciales;
- faire de la vente pyramidale;
- le minage de monnaie électronique;
- faire des envois massifs non autorisés.

4.2.15 Le corps professoral, le personnel enseignant, le personnel de recherche, les administrateurs, les administratrices et le personnel administratif peuvent faire un usage raisonnable et responsable à des fins personnelles de certaines technologies de l'information, notamment le poste de travail ou les appareils téléphoniques mis à sa disposition par l'Université. Cette utilisation ne doit pas affecter le fonctionnement, la sécurité ou l'intégrité des technologies de l'information de l'Université ni les informations qui y sont conservées.

4.3 Comportement numérique responsable

4.3.1 Les membres doivent participer activement aux activités d'éducation et de sensibilisation concernant l'adoption de comportements sécuritaires quant aux cybermenaces.

5. MESURES EXCEPTIONNELLES

Afin de maintenir la protection et de préserver l'intégrité des technologies de l'information de l'Université, les actions suivantes peuvent être effectuées :

- Interrompre ou révoquer temporairement les services offerts à une ou un membre afin de protéger les technologies de l'information;
- Intervenir sur une technologie de l'information suspectée de contrevenir à l'une ou l'autre des dispositions prévues dans le présent règlement;
- Appliquer les différentes fonctions de diagnostic sur les technologies de l'information;
- Prendre les actions nécessaires et requises afin de circonscrire une situation qui pourrait créer des préjudices graves à l'Université.

6. VÉRIFICATION DES TECHNOLOGIES DE L'INFORMATION

Tout en respectant la vie privée des personnes, l'Université se réserve le droit de faire des vérifications sur les technologies de l'information qu'elle administre et sur leur utilisation afin d'en assurer leur protection et leur bon fonctionnement tout au long de leur cycle de vie et de façon à ne pas compromettre ses activités.

7. SIGNALEMENT ET DÉNONCIATION

Les membres qui ont des motifs raisonnables de croire qu'une utilisation non conforme au présent règlement a été commise ou est en voie d'être commise doivent, dès que possible, signaler à l'Officière ou l'Officier de la sécurité de l'information et transmettre tous les renseignements et tous les documents disponibles et pertinents à la situation.

Les signalements et dénonciations seront traités en assurant leur confidentialité, sous réserve des lois, règlements et règles applicables.

8. SANCTIONS

Tout manquement au présent règlement peut entraîner, outre les mesures prévues aux législations, règlements, politiques, conventions ou ententes applicables, les conséquences suivantes, en fonction de la nature, de la gravité et des répercussions du geste ou de l'omission :

- Selon la gravité du manquement, le retrait ou l'annulation des privilèges d'accès aux technologies de l'information de l'Université. L'annulation peut être effectuée sans préavis.
- L'obligation de remboursement à l'Université de toute somme que cette dernière serait dans l'obligation de défrayer à la suite d'une utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses technologies de l'information.

9. DÉROGATION

Aucune dérogation au présent règlement n'est permise sans autorisation écrite de la vice-rectrice ou du vice-recteur aux infrastructures et à la transformation.

Toute demande de dérogation doit être acheminée à l'Officière ou l'Officier de la sécurité de l'information, qui se chargera de l'analyser et d'effectuer une recommandation auprès de la vice-rectrice ou du vice-recteur aux infrastructures et à la transformation qui prendra la décision d'approuver ou non la dérogation.

10. RÉVISION DU RÈGLEMENT

Le présent règlement est sous la responsabilité du vice-rectorat aux infrastructures et à la transformation. Il est révisé au besoin, mais au minimum tous les trois ans à compter de sa date d'adoption.

11. ADOPTION ET DATE D'ENTRÉE EN VIGUEUR

Le présent règlement entre en vigueur lors de son adoption par le Conseil d'administration.