Politique d'utilisation acceptable des services électroniques de l'UL

Instance administrative	Service de la technologie de l'information
Instance d'approbation	Vice-rectorat aux finances et à l'administration
Date d'approbation	ÉBAUCHE - en attente d'approbation finale
Dernière révision	6 février 2024
Prochaine révision	Février 2028
Historique des révisions	Octobre 2013, janvier 2015, septembre 2016, janvier 2018, février 2024

1. Objet

Cette politique a pour but d'assurer l'utilisation acceptable des services et dispositifs électroniques de l'Université Laurentienne (l'Université).

2. Portée

2.1 Cette politique s'applique à tous les utilisateurs des services de technologie de l'information (TI) de l'Université (annexe A), y compris la population étudiante, le corps professoral, le personnel, les invités, les affiliés, les partenaires et les organismes qui obtiennent des services de TI de l'Université. Elle s'applique également aux affiliés de l'Université (p. ex., partenaires, retraités, y compris les professeurs émérites, les entrepreneurs, etc.). Sa portée inclut :

2.1.1 l'observation de toutes les lois fédérales et provinciales et l'interdiction d'accomplir des activités illégales;

2.1.2 un processus pour lancer, revoir et approuver des politiques de TI;

2.1.3 l'élaboration et l'entretien de la TI;

2.1.4 la livraison de services électroniques qui fonctionnent comme il se doit (voir la liste des applications dans l'annexe A).

2.1.5 le fonctionnement et la conduite appropriés de l'Université concernant les services électroniques.

3. Définitions

3.1 **Renseignements confidentiels et personnels** s'entend des renseignements qui peuvent entraîner un préjudice pour l'Université, sa population étudiante, son corps professoral, son personnel ou d'autres entités ou particuliers s'ils sont divulgués de manière inappropriée, ou qui ne sont pas publics.

Exemples de renseignements confidentiels et personnels :

- un secret commercial, une propriété intellectuelle ou financière, des renseignements commerciaux, scientifiques ou techniques;
- des renseignements dont on pourrait raisonnablement s'attendre à ce que leur divulgation porte préjudice aux intérêts économiques de l'Université ou d'un autre établissement;
- des prises de position, des plans, des procédures, des critères ou des instructions à appliquer dans toute négociation menée ou à mener par ou au nom de l'Université;
- des plans concernant la gestion du personnel ou de l'administration de l'Université qui n'ont pas encore été appliqués ou rendus publics;
- des renseignements sur les employés, y compris sur la paie et la dotation en personnel.

3.2 **Renseignements personnels** s'entend de tout renseignement enregistré sur une personne identifiable, notamment :

- des renseignements concernant la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial ou familial de celle-ci;
- des renseignements concernant les études, les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels de cette personne ou des renseignements liés à sa participation à une opération financière;
- d'un numéro d'identification, d'un symbole ou d'un autre signe individuel qui lui est attribué;
- de l'adresse, du numéro de téléphone, des empreintes digitales ou du groupe sanguin de cette personne;
- de ses opinions ou de ses points de vue personnels, sauf s'ils se rapportent à une autre personne;
- de la correspondance ayant explicitement ou implicitement un caractère personnel et confidentiel adressée par la personne à un établissement, ainsi que des réponses à cette correspondance originale susceptibles d'en révéler le contenu;
- des opinions et des points de vue d'une autre personne au sujet de cette personne;
- du nom de la personne, s'il figure parmi d'autres renseignements personnels qui le concernent, ou si sa divulgation risque de révéler d'autres renseignements personnels au sujet de la personne (*Loi sur l'accès à l'information et la protection de la vie privée,* LRO 1990, Chap. F.31).

3.3 **Identificateur de l'UL** s'entend du nom d'utilisateur et du mot de passe qui donnent accès aux systèmes électroniques de l'Université.

3.4 **Dispositifs électroniques** s'entend des ordinateurs de bureau, des ordinateurs portables, des tablettes informatiques, des téléphones cellulaires et d'autres assistants numériques personnels.

3.5 **Services de la TI** s'entend du courrier électronique, de l'entreposage, des applications opérationnelles, des applications de collaboration, des systèmes d'enseignement et d'apprentissage, des systèmes de recherche et d'administration définis dans l'annexe A.

3.6 **Législation fédérale anti-pourriel** s'entend d'une loi visant à promouvoir la rentabilité et l'adaptabilité de l'économie canadienne en réglementant certaines activités qui découragent le recours aux moyens électroniques pour mener des activités commerciales, et modifiant la *Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes*, la *Loi sur la concurrence*, la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur les télécommunications* (L.C. 2010, ch. 23)

3.7 **Violation délibérée** s'entend d'une action enregistrée ou observée dans laquelle un changement de comportement dans nos systèmes déclencherait une action manuelle ou un avis d'un système surveillance (ou un billet).

3.8 **Zone publique** s'entend de toute zone intérieure ou extérieure ouverte à la communauté de l'Université (conformément à l'article 2.1) pour usage public.

3.9 **Acte inapproprié ou offensif** s'entend d'un acte, que ce soit un commentaire ou un comportement, qui dénigre ou est hostile à une personne ou montre de l'aversion et que toute personne pourrait raisonnablement percevoir comme perturbateur, irrespectueux, offensif ou inapproprié.

4. Énoncé de politique

4.1 L'Université reconnaît son obligation de protéger les renseignements personnels, la propriété intellectuelle et les droits d'accès des utilisateurs de l'Université.

4.2 Si les travaux de diagnostic et de maintenance effectués par le Service de la TI nécessitent l'accès à des fichiers ou données individuels et qu'il en résulte une violation des renseignements personnels, de la propriété intellectuelle et des droits d'accès, le VRA, Technologie de l'information, doit signaler l'incident au Bureau des affaires juridiques de l'Université.

4.3 Si les travaux de diagnostic et de maintenance effectués par le Service de la TI dévoilent des renseignements en violation de la *Loi sur l'accès à l'information et la protection de la vie privée*, le VRA, Technologie de l'information, doit signaler l'incident au Bureau des affaires juridiques de l'Université.

4.4 Le matériel de recherche et la propriété intellectuelle entreposés dans les systèmes de l'Université ou dans un système dans le nuage géré par l'Université sont traités conformément à la convention collective.

4.5 À l'exception des travaux de diagnostic et de maintenance effectués par le Service de la TI, l'accès aux dossiers électroniques n'est permis que lorsque la conseillère juridique générale déclare une circonstance exceptionnelle.

4.6 En cas d'incompatibilité entre cette politique et une convention collective quelconque, les dispositions de la convention collective ont préséance.

5. Utilisation de l'identificateur de l'UL et des services de technologie

5.1 L'Université a pour principe d'offrir un accès de qualité à ses systèmes électroniques aux personnes qui ont un identificateur valide de l'Université et aux visiteurs qui utilisent ses services (voir à l'annexe B les utilisations interdites des services de TI de l'Université).

5.2 Les services électroniques fournis par l'Université au corps professoral, au personnel, à la population étudiante et à d'autres membres de la communauté universitaire lui appartiennent et doivent être utilisés conformément à sa mission, aux normes de conduite honnête, responsable, professionnelle et respectueuse de l'éthique, être conformes à toutes les politiques et lignes directrices de l'Université, et ne pas lui causer de préjudice.

5.3 L'Université accepte un utilisateur lorsqu'il est approuvé par :

5.3.1 le secrétaire général quand il s'agit de la population étudiante;

5.3.2 le Service des ressources humaines quand il s'agit du personnel et du corps professoral.

5.4 L'Université désinscrit un utilisateur qui s'est séparé en permanence de l'Université :

5.4.1 Le secrétaire général désinscrit un membre de la population étudiante moins de 18 mois après :

- l'obtention du grade, ou
- être présumé inactif, ou
- a cessé sa relation avec l'Université, volontairement ou parce qu'il a été renvoyé.

5.4.2 Le Service des ressources humaines désinscrit les membres du personnel et les chargés de cours à une date qu'il définit et pour les raisons suivantes :

- décès,
- démission,
- départ à la retraite,
- cessation d'emploi.

5.4.3 Les membres à plein temps du corps professoral qui prennent leur retraite ou ont le titre de professeur émérite conservent un niveau modifié de services de TI décrit dans l'annexe D.

5.4.4 Le Service de la TI supprime le contenu du ou des comptes des utilisateurs au bout de dix mois d'inactivité après leur départ, sauf ceux des membres du PAPUL et de la haute direction (conservés durant dix ans).

5.4.5 Sauf lorsque le Service des ressources humaines ou le Bureau des affaires juridiques ou le secrétaire général autorise le maintien.

5.5 Les identificateurs et mots de passe de l'Université ne peuvent alors pas être réutilisés en dehors des systèmes officiels de l'Université, comme cela est indiqué dans l'annexe A.

6. Rôles et responsabilités

6.1 Le VRA, Technologie de l'information, a la responsabilité de faire appliquer les politiques touchant la TI, de promouvoir l'élaboration continue de ces politiques à l'Université et de faire approuver les normes ou lignes directrices nouvelles ou révisées par le Comité exécutif de gestion de la TI.

6.2 La gestion de la TI comprend :

6.2.1 Gestion de la stratégie de TI dirigée par le VRA, Technologie de l'information;

6.2.2 Gestion des données de la TI dirigée par le directeur des applications opérationnelles;

6.2.3 Gestion de la sécurité de la TI dirigée par le directeur du portfolio;

6.2.4 Gestion des projets de TI dirigée par le directeur du portfolio.

6.3 Le Comité exécutif de gestion supervise la gestion de la TI. Ce comité est constitué du VRA, Technologie de l'information, de la vice-rectrice aux finances et à l'administration, de la vice-rectrice principale aux études et de la vice-rectrice à la recherche.

6.4 Responsabilité de tous les titulaires d'identificateurs de l'UL

6.4.1 Il incombe au titulaire d'un identificateur d'informer immédiatement le Bureau des affaires juridiques et le Service de la TI de toute utilisation non autorisée de ses coordonnées (mot de passe, nom d'utilisateur ou jeton à plusieurs facteurs) en communiquant avec le service de dépannage de la TI (it@laurentian.ca ou poste 2200)

6.4.2 Protection des dispositifs électroniques :

6.4.2.1 Tous les dispositifs électroniques contenant des renseignements confidentiels ou personnels doivent être protégés par un mot de passe et s'éteindre automatiquement après 30 minutes d'inactivité ou d'absence de surveillance.

6.4.2.2 Les mots de passe ne peuvent pas être partagés.

6.4.2.3 Le Service de la TI doit encoder les renseignements confidentiels ou personnels entreposés dans des dispositifs électroniques, conformément à la Politique de gestion des informations numériques confidentielles.

6.4.2.4 La perte ou le vol de dispositifs et l'accès non autorisé à des dispositifs et services électroniques doivent être signalés immédiatement au Bureau des affaires juridiques et au VRA, Technologie de l'information.

6.5 Si l'Université soupçonne une violation de cette politique, elle peut lancer le processus d'atténuation (décrit dans l'annexe C).

7. Surveillance électronique de la conformité à cette politique

7.1 Afin d'assurer la sécurité de l'information et des systèmes, le Service de la TI surveille électroniquement l'utilisation des systèmes de l'Université par le corps professoral, le personnel, les entrepreneurs ou agents engagés par une unité ou un membre du personnel.

7.2 Le Service de la TI effectue cette surveillance au moyen de pistes de vérification de l'accès aux systèmes électroniques et d'examen périodique de ces pistes afin d'assurer la conformité à cette politique et la sécurité des informations que nous détenons.

7.3 Seuls les administrateurs des systèmes peuvent examiner les pistes de vérification en cas de nécessité absolue.

7.4 Consulter la Politique sur la surveillance électronique pour en savoir davantage sur la surveillance des systèmes d'information de l'Université.

Annexe A – Services électroniques de l'Université

Les services de TI de l'Université comprennent le courrier électronique, l'entreposage, les applications opérationnelles, les applications de collaboration, les systèmes d'enseignement et d'apprentissage ainsi que les systèmes de recherche et d'administration.

La liste complète des applications se trouve ici :
https://my.laurentian.ca/empl/en/learning?article=46105473 (EN)
https://my.laurentian.ca/empl/en/learning?article=46105475 (FR)

Annexe B – Utilisations interdites des services de TI de l'Université Laurentienne

L'Université Laurentienne interdit l'utilisation inappropriée des services électroniques, notamment :

a) Partager des mots de passe;

b) Essayer de commettre une infraction aux droits de propriété intellectuelle punissable en vertu du *Code criminel* du Canada;

c) Essayer de contourner toute mesure de sécurité ou de gestion des ressources;

d) Générer ou faciliter la génération de messages électroniques commerciaux non sollicités (pourriel). Ce type d'activité inclut entre autres :
    i. Envoyer des messages en contravention de la législation fédérale anti-pourriel, ou de toute autre loi anti-pourriel;
    ii. Imiter une autre personne ou usurper son identité ou son adresse électronique;
    iii. Créer de faux comptes dans le but d'envoyer des données de pourriel;
    iv. Fouiller dans toute propriété en ligne (de l'Université) pour trouver des adresses électroniques;
    v. Envoyer des messages électroniques non autorisés par l'entremise de serveurs ouverts de tiers;
    vi. Envoyer des messages électroniques, comme des courriels à des utilisateurs qui ont demandé d'être retirés d'une liste d'envoi.

e) Vendre, échanger ou distribuer à un tiers les adresses électroniques de toute personne, à son insu et sans son consentement permanent à cette divulgation;

f) Envoyer des messages non sollicités à un grand nombre d'adresses électroniques appartenant à des particuliers ou à des entités avec qui il n'existe pas de relations préétablies;

g) Envoyer, télécharger, distribuer, diffuser du contenu illégal, diffamatoire, harcelant, abusif, frauduleux, contrefait, obscène, pornographique, discriminatoire, haineux ou autrement répréhensible, ou offrir de le faire;

h) Distribuer intentionnellement des virus, des vers, des défauts, des chevaux de Troie, des fichiers corrompus, des canulars ou d'autres éléments de nature destructrice ou trompeuse;

i) Mener ou transmettre des ventes pyramidales et ce qui y ressemble;

j) Transmettre directement à un mineur du contenu qui peut lui être préjudiciable;

k) Essayer d'entraver la capacité des autres d'utiliser le réseau ou d'autres technologies communes;

l) Se faire passer pour une autre personne (en utilisant une adresse électronique ou d'une autre manière) ou se présenter faussement ou présenter faussement la source de tout message électronique et de tous autres services électroniques;

m) Transmettre illégalement la propriété intellectuelle ou d'autres renseignements exclusifs (de l'Université et d'autres) sans la permission du propriétaire de ces renseignements ou du titulaire de licence;

n) Essayer de découvrir ou de divulguer des renseignements confidentiels ou personnels entreposés dans les installations informatiques de l'Université;

o) Utiliser le courrier électronique de l'UL pour violer les droits juridiques (comme les droits à la confidentialité et à la publicité) des autres;

p) Promouvoir ou encourager une activité illégale;

q) Empêcher les autres utilisateurs de l'Université de profiter de tous ses services;

r) Créer divers comptes d'utilisateurs dans le cadre de la violation de cette politique ou créer des comptes d'utilisateurs par des moyens automatisés ou sous des prétextes frauduleux ou autres;

s) Vendre, échanger, revendre ou exploiter d'une autre façon tout compte de l'Université à des fins commerciales ou pour un transfert non autorisé;

t) Modifier, adapter, traduire ou effectuer des activités de rétro-ingénierie de toute partie des services de l'Université quand cela peut avoir des conséquences sur la continuité des affaires ou le rendement des services;

u) Reformater ou cadrer toute partie des pages Web qui font partie du service de l'Université;

v) Utiliser n'importe quel service de l'Université pour des communications illégales de fichiers entre pairs;

w) Vendre, échanger ou distribuer des produits ou services pour le seul profit personnel et sans profit pour l'Université;

x) Utiliser du contenu inapproprié, choquant ou pornographique dans des lieux publics où d'autres peuvent le voir sur l'écran d'un ordinateur ou d'autres dispositifs électroniques, et voir la personne qui regarde le contenu inapproprié, choquant ou pornographique;

y) Exploiter à des fins malintentionnées les vulnérabilités de matériel ou logiciel;

z) Utiliser une adresse électronique personnelle (qui n'est pas celle de l'Université) ou d'autres moyens numériques pour compromettre cette politique directement ou indirectement;

aa) Toute action ou activité qui contrevient aux politiques de l'Université, y compris la Politique pour un environnement respectueux de travail et d'étude, et le Code de conduite étudiante, le Code de conduite en matière de TI (pour le personnel de la TI), l'engagement en matière d'emploi à l'Université, et d'autres.

Annexe C – Processus d'atténuation en cas de violation de cette politique et processus d'appel

C.1.1 Si l'Université a des soupçons raisonnables de violation de la présente politique, elle est autorisée à :

a) Examiner les fichiers, programmes ou enregistrements électroniques de la ou des personnes, examen qui n'est pas nécessairement limité aux paramètres physiques des fichiers.
b) Supprimer temporairement les privilèges d'accès de la ou des personnes si une enquête plus poussée est justifiée, mais seulement après avoir fourni un avis de suspension et précisé le plan de l'enquête.

C.2 Lorsque la mauvaise utilisation est confirmée

C.2.1 Si l'Université détermine qu'une personne ou un programme lancé par une personne a délibérément violé cette politique, elle peut :

a) Lancer le processus de règlement de toute violation de la TI;
b) Demander au Bureau des affaires juridiques d'intervenir;
c) Supprimer l'accès de la personne aux installations et ressources électroniques.
d) Entreprendre des poursuites civiles si la mauvaise utilisation a porté préjudice à l'Université ou à tout membre de sa communauté, et si une intention ou un acte criminel est soupçonné.
e) Communiquer avec la police qui peut lancer des poursuites conformément au *Code criminel*.

C.3 Processus d'appel

C.3.1 Tout appel de la suppression de l'accès doit être adressé à la vice-rectrice aux finances et à l'administration en personne, par téléphone ou par courrier électronique de l'Université vpadmin@laurentian.ca) avec la mention APPEL PUA en objet.

Annexe D – Services de TI pour les membres à plein temps émérites et retraités du corps professoral

Les membres retraités du corps professoral (y compris émérites) conservent leur identificateur de l'Université et l'accès aux services suivants :

- Utilisation du même identificateur de l'Université;
- Authentification à plusieurs facteurs et la formation sur la cybersécurité;
- Services de Google for Education (Fundamentals), à savoir :
    - Google Mail, Docs, Slides, Sheets, Chat, Calendar, Meet (remplace Zoom);
    - Google Drive (+ Gmail) avec entreposage maximum de 50 Go;
- ma.Laurentienne;
- Bibliothèque;
- Logiciel de sécurité d'ordinateur de bureau (doit être conforme à la norme informatique de l'Université; appeler ou écrire au service de dépannage de la TI);
- Doivent observer la Politique sur l'utilisation acceptable et d'autres politiques de l'Université touchant la TI;
- Soutien du service de dépannage pour les services indiqués ci-dessus.

Obligations

Les membres retraités du corps professoral qui conservent des privilèges de TI doivent se conformer à cette politique et à d'autres politiques de TI et suivre la formation obligatoire sur la cybersécurité ainsi que d'autres formations sur les systèmes numériques requis (et communiqués).