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

Instance administrative	Bureau du dirigeant principal de l'information
Instance d'approbation	Équipe de gestion
Date d'approbation	8 décembre 2017
Dernière révision	28 novembre 2017
Prochaine révision	Novembre 2022

1. Objet

1.1 Cette politique a pour but de régir l'utilisation des services électroniques de l'Université Laurentienne et de :

1.1.1 définir clairement ce qui constitue un usage approprié des services électroniques de l'Université Laurentienne;
1.1.2 fournir des renseignements clairs sur les conséquences de la violation de cette politique;
1.1.3 donner à cette politique préséance sur tous autres énoncés et politiques d'utilisation acceptable.

2. Portée

2.1 Cette politique s'applique à tous les utilisateurs des ressources de la technologie de l'information (TI) de l'UL et couvre :

2.1.1 la structure et les critères de ce qui peut entrer dans la catégorie des politiques, lignes directrices ou normes de la TI;
2.1.2 l'observation de toutes les lois fédérales et provinciales et l'interdiction d'accomplir des activités illégales;
2.1.3 un processus pour lancer, revoir, approuver et supprimer des politiques de TI;
2.1.4 l'élaboration et l'entretien de la TI;
2.1.5 la livraison de services électroniques qui fonctionnent comme il se doit (voir la liste des applications à l'annexe A).

3. Définitions

3.1 Les définitions qui font partie de cette politique se trouvent à l'annexe B.

4. Déclaration concernant l'accès aux renseignements et leur divulgation à L'Université Laurentienne

4.1 L'Université Laurentienne reconnaît son obligation de respecter la confidentialité, la propriété intellectuelle et les droits d'accès des utilisateurs de l'Université Laurentienne.

4.2 Si les travaux de diagnostic et de maintenance que fait le Service de la TI nécessitent l'accès à des fichiers ou données individuels et qu'il en résulte une violation de la confidentialité, de la propriété intellectuelle et des droits d'accès, le dirigeant principal de l'information doit signaler l'incident à la conseillère juridique de l'Université ou à son délégué, et l'agent responsable de la protection de la vie privée avertira la ou les personnes concernées.

4.3 Si les travaux de diagnostic et de maintenance que fait le Service de la TI exposent des informations en violation de la LAIPVP ou des droits de la personne, le dirigeant principal de l'information doit signaler le cas à la conseillère juridique de l'Université ou à son délégué.

4.4 Les documents de recherche de même que la propriété intellectuelle stockés sur les systèmes de l'UL restent la propriété de l'auteur.

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

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

5. Utilisation de l'identificateur de l'UL et les Services de technologie

5.1 Les politiques de la TI soulignent la gestion et l'utilisation de la technologie de l'information, et appuient les missions fondamentales de recherche, d'enseignement et d'apprentissage de l'Université Laurentienne.

5.2 L'Université Laurentienne a pour principe d'offrir un accès de qualité à ses systèmes électroniques aux personnes qui ont un identificateur valide de l'UL et aux visiteurs qui utilisent ses services (voir à l'annexe C les utilisations interdites du Service de la TI de l'UL).

5.3 Les services électroniques fournis par l'Université 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.

6. Rôles et responsabilités

6.1 Le dirigeant principal de l'information a la responsabilité de faire appliquer les politiques de la TI, de promouvoir l'élaboration continue de politiques de la TI à l'UL et de faire approuver les normes ou lignes directrices nouvelles ou révisées par l'Équipe de gestion de l'UL.

6.2 Le Comité de gouvernance de la TI est composé de membres de la communauté de l'UL et fournit au dirigeant principal de l'information un examen objectif et des recommandations pertinentes de modification du texte des politiques de la TI et des priorités en matière de TI.

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

6.3.1 Le titulaire d'un identificateur de l'UL doit signaler immédiatement au Service de la TI toute utilisation non autorisée de son mot de passe ou de son compte (p. ex., par un ami, un parent, un collègue, etc.) en appelant le comptoir de dépannage du Service de la TI au poste 2200 ou en écrivant à it@laurentian.ca.

6.3.2 Protection des dispositifs électroniques

6.3.2.1 Tous les dispositifs électroniques contenant des renseignements confidentiels doivent être protégés par un mot de passe et s'éteindre automatiquement après une certaine période d'inactivité.

6.3.2.2 Le Service de la TI doit encoder les renseignements confidentiels entreposés dans des dispositifs électroniques, conformément à la politique de gestion des informations numériques confidentielles.

6.3.2.3 La perte et le vol de dispositifs et l'accès non autorisé à des dispositifs et services électroniques doivent être signalés immédiatement au Secrétariat de l'Université et au Bureau du dirigeant principal de l'information.

6.4 Si l'Université soupçonne une violation de cette politique, elle peut lancer le processus (voir le processus à l'annexe D).

Annexe A – Services électroniques de l'UL

Liste des services de l'UL

- Courrier électronique, Gmail
- LUnet, MaLaurentienne
- Google Drive, Apps et applications de Google
- Système de gestion de l'apprentissage (SGA) (p. ex., D2L)
- CarteBlanche
- Bibliothèque avec accès par procuration
- Système sans fil
- WebAdvisor
- Ellucian's Colleague et services auxiliaires (p. ex., Synoptyx, CROA, etc.),
- Tableau
- Comptes de médias sociaux de l'UL
- FUSION et services auxiliaires (p. ex., SugarCRM, etc.),
- Evernote
- Accès à Internet
- Autres services électroniques gérés par le Service de la TI de l'UL comme REDCAP, Zoom, FTP et d'autres.

Annexe B - Définitions

Accès par procuration – S'entend du système d'accès en ligne à la Bibliothèque.

Courrier électronique – S'entend de GroupWise, LU Webmail, Google Apps et de tous les autres services officiels de courrier électronique de l'UL.

Dispositifs électroniques – S'entend des ordinateurs de bureau, des ordinateurs portables, des tablettes informatiques, des téléphones cellulaires, des BlackBerry et d'autres assistants numériques personnels.

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

LUNET – S'entend de l'intranet de l'Université Laurentienne.

Renseignements confidentiels – S'entend de tout renseignement qui ne doit pas être rendu public.

Renseignements personnels – S'entend des renseignements consignés ayant trait à un particulier qui peut être identifié. S'entend 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 celui-ci;
- des renseignements concernant les études, les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels de ce particulier 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 ce particulier;
- de ses opinions ou de ses points de vue personnels, sauf s'ils se rapportent à un autre particulier;
- de la correspondance ayant explicitement ou implicitement un caractère personnel et confidentiel, adressée par le particulier 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 ce particulier;
- du nom du particulier, s'il figure parmi d'autres renseignements personnels qui le concernent, ou si sa divulgation risque de révéler d'autres

renseignements personnels au sujet du particulier (*Loi sur l'accès à l'information et la protection de la vie privée,* art. 2).

Réseau local – S'entend du réseau câblé.

Sans fil de l'UL – S'entend du réseau local sans fil du campus pour accéder à Internet et aux services sans fil indiqués dans cette politique.

SGA – S'entend du système de gestion de l'apprentissage.

WebAdvisor – S'entend du portail administratif des étudiants de l'UL.

Annexe C – Usages interdits des services de TI de l'UL

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

a) Communiquer 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 électroniques contrairement à la *CAN-SPAM Act* ou à toute autre loi antipourriel applicable. 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'UL) 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 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 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'UL 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 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'UL 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'UL 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'UL 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'UL.
v) Utiliser n'importe quel service de l'UL 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'UL.
x) Utiliser du contenu inapproprié, choquant ou pornographique dans des lieux publics où d'autres peuvent le voir sur l'écran de l'ordinateur ou d'autres dispositifs électroniques, et voir la personne qui regarde le contenu inapproprié.
y) Exploiter à des fins malintentionnées les vulnérabilités de matériel ou logiciel.
z) 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 de la population étudiante.

Annexe D – Marche à suivre en cas de violation de cette politique et processus d'appel

D.1 En cas de soupçon de mauvaise utilisation

D.1.1 Si l'Université a des motifs raisonnables de soupçonner une violation de cette 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.

D.2 Quand la mauvaise utilisation est confirmée

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

a) Supprimer l'accès de cette personne aux installations et ressources électroniques.
b) 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.
c) Communiquer avec la police qui peut lancer des poursuites conformément au *Code criminel*.

D.3 Processus d'appel

D.3.1 Tout appel de la suppression de l'accès doit être adressé à la vice-rectrice à l'administration en personne, par téléphone ou par courrier électronique personnel avec la mention APPEL PUA en objet.