Politique de gestion de l'information numérique confidentielle

Instance administrative :	Service de la technologie de l'information
Instances d'approbation :	Rectorat et Équipe de gestion
Date d'approbation :	23 avril 2019
Prochaine révision :	Juin 2022
Historique des révisions :	Avril 2015, Avril 2019

1. Objet

1.1 Conjointement avec les principes énoncés dans la Politique de l'Université Laurentienne sur l'accès à l'information et la protection de la vie privée, l'objet de la Politique de l'Université Laurentienne sur la gestion de l'information numérique confidentielle (« la Politique ») est de :

1.1.1 protéger la confidentialité, l'intégrité et la disponibilité de l'information numérique confidentielle;

1.1.2 stipuler, de clarifier et de définir le mode autorisé de stockage et de transmission numériques de données dans le souci de gérer et d'atténuer efficacement le risque de stockage et de transmission non autorisés d'information numérique confidentielle de même que de prévenir les risques à l'endroit de l'Université Laurentienne de Sudbury (« l'Université ») et visés par la *Loi sur l'accès à l'information et la protection de la vie privée*.

2. Étendue

2.1 Cette politique s'applique à l'ensemble des membres de l'administration, du corps professoral, du personnel et de la population étudiante employés par la Laurentienne, aux bénévoles de l'Université, de même qu'à tous les établissements affiliés, qui pourraient, dans le cadre de leurs rôles et responsabilités, stocker et transmettre par voie numérique de l'information confidentielle.

2.2 Quiconque crée, utilise, traite, stocke, transfère, administre et (ou) détruit de l'information numérique confidentielle est responsable de la conformité à cette politique.

2.3 Quel que soit le support de stockage des données, l'Université a des obligations juridiques et éthiques afin d'assurer que ces données sont gérées d'une manière qui en maximise l'utilité tout en minimisant les risques d'utilisation ou de divulgation non autorisée ou inappropriée.

2.4 Cette politique n'aborde pas les droits de la personne en ce qui a trait au droit d'auteur ou aux droits de propriété intellectuelle.

3. Définitions

3.1 « Information numérique confidentielle » s'entend de l'information concernant :

3.1.1 Une personne identifiable, notamment :

3.1.1.1 des données biologiques et signalétiques comme des informations relatives à la race, la nationalité ou l'origine ethnique, la couleur, la religion, l'âge, le sexe, l'identification du sexe, l'orientation sexuelle ou le statut matrimonial ou familial de la personne, le groupe sanguin, les empreintes numériques, etc.;

3.1.1.2 les informations relatives aux transactions financières que la personne a eues avec l'Université, comme les transactions par carte de crédit et le solde du compte;
3.1.1.3 les informations relatives à la scolarité ou aux antécédents professionnels de la personne;
3.1.1.4 les informations relatives aux antécédents médicaux, psychiatriques, psychologiques ou criminels de la personne;
3.1.1.5 tout numéro identificateur, symbole ou autre élément qui lui est propre comme un numéro d'étudiant ou d'employé;
3.1.1.6 les coordonnées comme l'adresse, le numéro de téléphone, l'adresse électronique et l'identité électronique personnelle de la personne;
3.1.1.7 les opinions ou points de vue personnels de la personne, sauf s'ils se rapportent à une autre personne;
3.1.1.8 toute correspondance envoyée à l'Université par la personne, qui est implicitement ou explicitement de nature privée ou confidentielle, et toute réponse à cette correspondance qui pourrait révéler le contenu de la correspondance d'origine;
3.1.1.9 les idées ou opinions d'autrui concernant la personne;
3.1.1.10 le nom de la personne s'il figure dans d'autres informations privées la concernant ou lorsque la divulgation du nom révélerait d'autres informations privées sur celle-ci;

3.1.2 Documents identifiables de l'Université réputés non publics et traités comme des informations confidentielles;

3.1.3 Identifiants confidentiels attribués par le gouvernement, y compris les suivants :
3.1.3.1 le numéro d'assurance sociale, le numéro de sécurité sociale, la carte de santé et le permis de conduire.

3.2 « Registre », « données » et « renseignement » désignent toute information, quelle que soit la manière dont elle est consignée ou copiée, que ce soit sous une forme imprimée, sur film, par des moyens électroniques (numérique et analogique) ou autre, et comprend :
3.2.1 des lettres, une note de service, un livre, un plan, une carte, un dessin, un schéma, une œuvre picturale ou graphique, une photographie, un film, un microfilm, un enregistrement sonore, une vidéo, un enregistrement lisible par machine, un autre matériel documentaire, quelle qu'en soit la forme ou les caractéristiques physiques, et toute reproduction de ces éléments;
3.2.2 tout enregistrement ou toute donnée qui peut être produit(e) à partir d'un document lisible par machine, sous le contrôle de l'Université, au moyen de matériel ou logiciel ou tout autre équipement de stockage de l'information.

3.3 « Stockage infonuagique » signifie toute information, quelle que soit la manière dont elle est consignée, que ce soit sous une forme imprimée, sur film, par des moyens électroniques ou autre, qui est stockée numériquement sur un périphérique, un support ou un service, y compris les moyens suivants :
3.3.1 centres de données de l'UL;
3.3.2 ordinateur;
3.3.3 périphérique de stockage amovible;
3.3.4 le nuage (Internet);
3.3.5 courriel;
3.3.6 logiciel;
3.3.7 tout autre dispositif électronique qui peut stocker de l'information.

3.4 « Mémoire d'ordinateur » désigne toute information, quelle que soit la manière dont elle est consignée, que ce soit sous une forme imprimée, sur film, par des moyens électroniques ou autre, qui est stockée numériquement sur un périphérique, un support ou un ordinateur, y compris les suivants :

3.4.1 ordinateur de bureau et ordinateur portable;
3.4.2 périphérique de stockage amovible;
3.4.3 appareil mobile comme un cellulaire.

3.5 « Stockage permanent » signifie toute information, quelle que soit la manière dont elle est consignée, que ce soit sous une forme imprimée, sur film, par des moyens électroniques ou autres, qui est stockée numériquement pendant plus de cinq (5) jours.

3.6 « Stockage temporaire » signifie toute information, quelle que soit la manière dont elle est consignée, que ce soit sous une forme imprimée, sur film, par des moyens électroniques ou autres, qui est stockée numériquement pendant moins de cinq (5) jours consécutifs.

3.7 « Transmission » et « transmission de données » s'entendent du transfert d'information par voie numérique d'un support à l'autre et qui peut être désigné comme :

3.7.1 envoi;
3.7.2 transfert;
3.7.3 soumission;
3.7.4 échange;
3.7.5 téléchargement;
3.7.6 partage;
3.7.7 autres descriptions assimilées à la transmission.

3.8 « Périphérique de stockage amovible » s'entend de tout type de dispositif de stockage qui peut être enlevé d'un ordinateur ou d'un téléphone mobile, alors même que le système est en marche, y compris les éléments suivants :

3.8.1 clé USB, clé USB portable et clé de mémoire;
3.8.2 disquette ou support de stockage magnétique comme une bande;
3.8.3 disque dur portable ou amovible;
3.8.4 disque optique comme un CD, DVD, disque Blu-Ray;
3.8.5 autres périphériques de stockage amovibles.

3.9 « Identifiants de l'UL » désignent le nom d'utilisateur et le mot de passe que vous avez à l'Université Laurentienne et qui sont gérés par l'Université et la Politique régissant les mots de passe.

3.10 « Services approuvés par l'UL » s'entendent des applications gérées ou sanctionnées par l'Université, ces services nécessitant ordinairement des identifiants d'accès conformes à la Politique de l'Université régissant les mots de passe et comprennent, sans s'y limiter, les installations suivantes :

3.10.1 maLaurentienne, LUNET, SecureFA et d'autres portails Web de la Laurentienne;
3.10.2 D2L;

3.10.3 Google G Suite gérée par l'UL (identifiants d'accès de l'UL nécessaires), y compris Gmail, Google Doc, Google Sheets, et les autres applications de G Suite gérées par la Laurentienne;
3.10.4 Colleague, WebAdvisor, Self Service (p. ex., planification de la population étudiante) et logiciels associés (p. ex., Synoptic, CROA/Business Objects, etc.);
3.10.5 SugarCRM, Fusion, Marketo;
3.10.6 Avaya, Avotus ICM, Zoom;
3.10.7 REDCap;
3.10.8 Orbis et autres plateformes approuvées d'apprentissage par l'expérience;
3.10.9 autres services de l'UL approuvés.

3.11 Si un logiciel ou un service quelconque ne figure pas dans cette politique ou sur le site intranet du Service de la TI, il est possible de demander ce logiciel ou ce service auprès du Service de la TI (it@laurentian.ca). Chaque demande sera sérieusement examinée.

3.12 Le service non géré et les services infonuagiques non gérés sont des services qui ne sont ni administrés ni sanctionnés par le Service de la TI, et ne figurent pas dans la liste à l'article 3.10. Il peut s'agir, par exemple, de :
3.12.1 Dropbox;
3.12.2 Google Drive et Google Docs (sauf s'ils sont gérés par l'UL);
3.12.3 Microsoft 365;
3.12.4 Apple iCloud;
3.12.5 Amazon Storage;
3.12.6 applications Web;
3.12.7 applications mobiles;
3.12.8 tous les autres services non sanctionnés.

4 Gestion d'information numérique confidentielle

4.1 Stockage
4.1.1 L'information numérique confidentielle doit seulement être stockée de manière permanente sur les services gérés par l'Université, comme décrits à l'article 3.10.
4.1.2 L'information numérique confidentielle peut seulement être stockée de manière temporaire sur la mémoire d'ordinateur (comme défini à l'article 3.4) protégé par un mot de passe et conforme à la Politique de l'Université régissant les mots de passe.
4.1.3 L'information numérique confidentielle ne doit pas être stockée de manière permanente sur la mémoire d'ordinateur, comme défini à l'article 3.4.
4.1.4 L'information numérique confidentielle ne doit pas être stockée de manière temporaire ou permanente sur les services infonuagiques non gérés.

4.2 Transmission
4.2.1 La transmission d'information numérique confidentielle est autorisée dans les limites du campus de l'Université (réseaux câblés et sans fil).
4.2.1.1 La transmission d'information numérique confidentielle au-delà du campus de l'Université n'est autorisée que pour les applications et services réputés conformes à l'article 4.1, et cette transmission est autorisée si elle se limite aux protocoles sécurisés utilisant le protocole de transfert HTTPS (HTTP sécurisé) ou se fait par l'entremise d'un réseau privé virtuel approuvé (VPN).
4.2.2 La transmission d'information numérique confidentielle n'est pas autorisée vers les services infonuagiques non gérés, y compris les sites de médias sociaux.

4.2.3 La transmission d'information numérique confidentielle n'est pas autorisée au moyen d'un service non géré comme un système de messagerie mobile (SMS), sauf dans le cas de services sécurisés et cryptés gérés par la Laurentienne.

4.3 Logiciels antivirus et anti-mouchards

4.3.1 Tous les ordinateurs de bureau et les ordinateurs portables payés par l'UL doivent être équipés à tout moment de logiciels antivirus et anti-mouchards approuvés par le Service de la TI selon le type de périphérique et les spécifications définies.

4.4 Envoi de messages électroniques

4.4.1 Les adresses électroniques deviennent confidentielles quand une longue liste de destinataires (plus de 50) peut être contextualisée, comme les adresses associées à l'Université, ou une longue liste associée à une unité d'enseignement, etc.

4.4.1.1 Un message électronique destiné à une liste de 100 destinataires ou plus doit être envoyé en tant que « Cci » (copie conforme invisible) plutôt qu'en indiquant les destinataires dans le champ « Destinataires ».

4.4.1.2 Il est recommandé d'envoyer un message électronique destiné à plus de 50, mais moins de 100 destinataires en tant que « Cci ».

4.5 Élimination de l'information numérique confidentielle

4.5.1 Tous les périphériques numériques ou analogiques qui contiennent en ce moment ou contenaient de l'information numérique confidentielle doivent être supprimés en toute sécurité, par le Service de la TI; il faut communiquer avec le comptoir de service de la TI à ces fins.

4.5.2 Toutes les mémoires d'ordinateur ou périphériques qui ont entreposé temporairement de l'information numérique confidentielle doivent être supprimées (et la corbeille vidée) dans l'espace de cinq (5) jours.

4.6 Les logiciels et services qui entreposeront l'information numérique confidentielle doivent être approuvés et administrés par le Service de la TI et toute dérogation doit être approuvée par le vice-recteur associé à la technologie de l'information.

5 Conformité

5.1 Les mesures disciplinaires ou autres peuvent s'imposer dans les cas où les pratiques de travail ou d'autres activités sont contraires à cette politique ou non conformes à celle-ci et dans le respect des droits et obligations établis par les conventions collectives et la politique de l'Université.

5.2 Toute demande d'exceptions aux exigences énoncées dans cette politique doit être faite, par écrit, au vice-recteur associé à la technologie de l'information, qui pourrait consulter la secrétaire de l'Université et conseillère générale.