Université de l'Ontario français

Numéro du document normatif	
Instance d'approbation	Conseil de gouvernance
Responsabilité administrative	Vice-recteur à l'administration
Date d'approbation	21 décembre 2021
Date d'entrée en vigueur	21 décembre 2021
Date de dernière révision	

Politique sur la sécurité de l'information numérique

1. Préambule

Dans l'accomplissement de sa mission, l'Université de l'Ontario français (ci-après « l'Université ») traite de l'information sous plusieurs formes et sur plusieurs supports à l'aide de différents systèmes d'information. L'information détenue par l'Université afin de soutenir ses activités possède une valeur administrative, légale, financière ou patrimoniale et doit, par conséquent, faire l'objet d'une évaluation continue, d'une utilisation appropriée et d'une protection adéquate tout au long de son cycle de vie. À ces fins, la mise en œuvre d'un ensemble cohérent de mesures de sécurité, déterminé par une approche de gestion des risques, est nécessaire.

2. Objectif

La présente politique vise à faire de l'Université une institution protégée, résiliente et proactive en matière de sécurité de l'information qui offre des services numériques de qualité aux membres de la communauté universitaire. Son objectif est d'affirmer l'engagement de l'Université à assurer la sécurité de l'information, et ce, conformément aux lois, politiques et règlements applicables. Plus précisément, elle vise à :

a) garantir la mise en place de mécanismes de contrôle appropriés en matière de disponibilité, d'accessibilité, d'intégrité et de confidentialité de l'information, y compris les données de recherche;
b) préciser les rôles et les responsabilités de tous les acteurs impliqués dans la sécurité de l'information de l'Université;
c) favoriser et encourager l'adoption de comportements sécuritaires auprès des utilisatrices et des utilisateurs de l'Université.

3. Champ d'application et portée

La présente politique s'applique à l'ensemble des utilisatrices ou utilisateurs de l'Université. Elle régit toute information détenue, recueillie, conservée, transmise ou produite par l'Université ou une tierce partie, conseil, fournisseur ou autre partenaire externe, sous forme numérique, et pour l'intégralité du cycle de vie de ladite information.

4. Valeurs et principes d'application

Les principes d'application suivants guident les actions de l'Université en matière de sécurité de l'information :

a) de s'appuyer sur les normes pertinentes afin de favoriser le déploiement des meilleures pratiques utilisées dans des organismes ou établissements similaires;

b) d'identifier les mesures de sécurité de l'information en fonction de son degré de sensibilité et des risques et menaces pouvant affecter sa disponibilité, son intégrité et sa confidentialité. Ces mesures doivent couvrir la protection de l'information, la détection de tout usage abusif ou inapproprié de l'information, l'élimination des menaces et le recouvrement des activités de l'Université possiblement compromises;

c) de déployer des mesures de sécurité adéquates et cohérentes permettant d'atténuer les risques et de les maintenir à un niveau acceptable;

d) de protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;

e) de se prémunir contre les interruptions de service en disposant de plans de continuité et de relève permettant d'assurer la remise en opération des services jugés essentiels en cas d'incident majeur de sécurité de l'information; et

f) de promouvoir de bonnes pratiques de protection des actifs informationnels, notamment par l'élaboration et la diffusion d'activités de sensibilisation et de perfectionnement du personnel de l'Université.

5. Définitions

Pour les besoins de la présente politique, les définitions suivantes s'appliquent :

a) Actif informationnel : tout bien matériel ou numérique qui sert à enregistrer, entreposer, à utiliser, à transmettre ou à recevoir de l'information ou qui permet son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue de celle-ci. Au nombre des actifs on y retrouve notamment : les applications, les bases de données, les serveurs, les ordinateurs portables et les cellulaires.

b) Administratrices et administrateurs des données : les personnes qui assurent la supervision de l'information.

c) Cyber-attaque: une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants.

d) Entrepôt de données : un répertoire central qui a pour objet de faciliter l'accès aux données à des fins décisionnelles. Il contient des informations sur de nombreux sujets et provenant de sources multiples.

e) Gardienne désignée ou gardien désigné : l'unité ou la personne qui est responsable d'un actif et qui doit procéder régulièrement à des examens de la conformité de celui-ci à la présente politique et à l'ensemble des lignes directrices et structures applicables. Elle ou il en assure la supervision de l'information connexe.

f) Gouvernance des données : un ensemble de normes et de processus liés à la gestion des données qui sont suivis par tous les utilisatrices ou utilisateurs et qui assurent l'exactitude, l'intégrité et l'accessibilité de l'information.

g) Information : les données institutionnelles qui sont toute représentation ou description normalisée de faits ou de chiffres pouvant être créées, recueillies, traitées, communiquées ou interprétées, ainsi que les données personnelles qui permettent d'identifier une personne.

h) Programme de sécurité de l'information : un ensemble de projets, de formations et de mesures mis en œuvre pour remédier à toute lacune actuelle en matière de sécurité de l'information, répondre à toute nouvelle menace pour la sécurité, revoir les normes et mettre en place des processus afin d'atteindre et de maintenir le niveau de sécurité visé.

i) Utilisatrice ou utilisateur : toute personne ayant accès à l'information de l'Université, ceci inclus tous les membres du corps professoral, du personnel, des étudiantes et des étudiants, des diplômées et des diplômés, des locataires et des visiteurs ainsi qu'à toute personne autorisée à utiliser les installations numériques de l'Université

6. Gestion de la sécurité de l'information

La gestion de la sécurité de l'information inclut les principes suivants :

a) le développement d'un ensemble de compétences organisationnelles afin de gérer le risque en matière de sécurité de l'information à l'échelle de l'Université;

b) la création d'une culture axée sur la sécurité de l'information au sein de la communauté et la définition des responsabilités en matière de sécurité de l'information incombant à tous les utilisatrices ou utilisateurs;

c) la sécurisation et la protection de tout actif ayant trait à la sécurité de l'information;

d) la gestion de l'accès à l'information et l'utilisation responsable des systèmes, et ce, conformément aux dispositions des politiques de l'Université en la matière;

e) l'élaboration et la mise en œuvre de directives, de règles, de procédures, de principes directeurs et de pratiques exemplaires en matière de sécurité de l'information, comme le déterminent la chef ou le chef de l'information et la chef ou le chef de la sécurité de l'information avec l'appui des membres de la haute direction, et ce, conformément aux politiques de l'Université et aux lois et aux normes applicables;

f) la conception et la conservation de l'information conformément aux politiques et procédures de l'Université, ainsi que les lois et règlements applicables;

g) le répertoriage et la classification de l'information assujettie à la présente politique;

h) la gestion des risques, l'assignation de niveaux de sécurité et la vérification de la conformité des processus en fonction des degrés de risque et de confidentialité associés à l'information en question;

i) l'offre de soutien, de renseignements et d'activités de formation en matière de sécurité de l'information aux unités et aux utilisatrices ou utilisateurs;

j) le suivi, la vérification et la mise à l'épreuve de la sécurité des systèmes d'information et, s'il y a lieu, la réévaluation des besoins, des règles et des responsabilités;

k) l'élaboration et la mise en œuvre de procédures de détection des menaces en matière de sécurité de l'information et l'apport rapide et responsable de solutions à tout incident ou infraction ayant trait à la sécurité de l'information; et

l) la mise en application des présentes mesures ainsi que des politiques et directives connexes de l'Université.

7. Rôles et responsabilités

7.1. La mise en œuvre, incluant toute révision de la présente politique, relève du vice-rectorat à l'administration.

7.2. Sous l'autorité du vice-rectorat à l'administration, la direction de la Stratégie numérique est responsable de l'élaboration des politiques, procédures, lignes directrices et solutions technologiques de l'Université associées à la sécurité de l'information. Elle participe en outre à leur mise en œuvre à l'échelle de l'Université.

7.3. Sous l'autorité de la direction de la Stratégie numérique, le personnel de la stratégie numérique élabore et exécute des plans stratégiques et opérationnels opportuns. Il participe également à la mise en œuvre des politiques, procédures, lignes directrices et solutions technologiques de l'Université associées à la sécurité de l'information. Enfin, il assure la liaison avec les partenaires intéressés, à l'interne comme à l'externe, pour les questions liées à la sécurité de l'information.

7.4. En vue de faciliter la mise en œuvre de la présente politique, des procédures, des guides, des processus ou d'autres documents peuvent être rédigés.

Les sujets suivants peuvent faire l'objet de ce travail :

a) les procédures et lignes directrices sur l'utilisation de l'infonuagique;
b) la gestion des identités et des accès, notamment les procédures et lignes directrices relatives à la gestion des mots de passe;
c) les procédures et lignes directrices sur la gestion des sauvegardes; et
d) le développement de la gouvernance des données

7.5. Il incombe au vice-rectorat à l'administration de s'assurer que les employées et employés ainsi que toute autre personne qu'elle ou il encadre sont informés de la présente politique et des responsabilités qui y sont énoncées.

7.6. Il incombe au vice-rectorat à l'administration ainsi qu'à la direction de la stratégie numérique de coordonner leurs efforts à ceux que déploient, dans le cadre de diverses initiatives, les comités pertinents de l'Université.

Le Comité directeur des technologies numériques de l'information est doté de responsabilités et de mandat spécifiques portant sur :

- le maintien de la sécurité de l'information;
- la garantie de la sécurité des actifs;
- la réponse à toute atteinte à la protection des renseignements personnels;
- la prévention de la fraude; et
- la résolution des incidents en matière de sécurité de l'information.

Le mandat, la composition et la structure de ce comité peuvent être modifiés, complétés au fil du besoin par d'autres comités ou équipes d'intervention.

7.7. La direction de la stratégie numérique s'assure que la conception, la configuration, la mise en œuvre, l'exploitation, l'entretien, la mise à jour et la mise hors service des systèmes se déroulent selon les besoins déterminés en matière de sécurité de l'information.

7.8. Il incombe aux administratrices et administrateurs de système ou d'application de configurer les dispositifs de sécurité des actifs qu'ils gèrent conformément aux politiques, aux procédures, aux lignes directrices et aux diverses exigences de l'Université. Tout actif intégrant des paramètres de sécurité susceptibles d'être configurés ou modifiés doit être assigné à une administratrice ou à un administrateur.

7.9. Il incombe aux administratrices et administrateurs des données de s'assurer de l'exactitude de l'information, de son accessibilité à tout utilisatrice ou utilisateur autorisé et de sa classification conformément aux politiques et directives de l'Université, notamment la Politique sur la gouvernance des données privées et le cadre de gouvernance des données.

7.10. Il incombe aux membres de l'équipe responsable de la sécurité aux services des technologies de l'information et aux administratrices et administrateurs des données de s'assurer que les systèmes sont évalués aux fins des exigences relatives à la sécurité de l'information, et ce, à intervalles réguliers et en conformité avec les directives des instances gouvernementales pertinentes.

7.11. Tout actif doit être confié à une gardienne ou à un gardien désigné, qu'il appartienne à l'Université ou autre. Il incombe à cette personne de veiller au respect de la présente politique.

7.12. L'utilisatrice ou l'utilisateur est tenu:

a) de se conformer à la présente politique et à l'ensemble des exigences relatives à la sécurité de l'information qui y sont stipulées de même qu'à toute autre politique connexe de l'Université, y compris les procédures, règles, consignes et principes directeurs y afférents;
b) de suivre une formation sur la sécurité de l'information;
c) d'assurer la protection de tout mot de passe ou accès que lui fournit les services des technologies de l'information ou une administratrice ou un administrateur de système. Le droit d'accès est restreint à la personne qui en bénéficie, et une autre utilisatrice ou un autre utilisateur ne peut s'en prévaloir;
d) de prendre les mesures appropriées afin d'éviter que tout actif placé sous sa responsabilité soit perdu, endommagé ou utilisé abusivement ou qu'il fasse l'objet d'un accès non autorisé;
e) de respecter la classification prévue de l'information; et
f) de signaler rapidement tout acte associé à une infraction, réelle ou présumée, à la sécurité, y compris, mais sans s'y limiter, l'accès non autorisé, le vol, l'intrusion informatique, le vandalisme et la fraude.

8. Non-conformité

8.1. La non-conformité à la présente politique peut entraîner diverses sanctions, incluant la suspension immédiate du droit d'accès de l'utilisateur à un ou à plusieurs systèmes, la résiliation de l'accès aux systèmes d'information de l'Université et toute autre mesure disciplinaire jugée appropriée dans les circonstances.

8.2. L'utilisatrice ou l'utilisateur engage sa responsabilité personnelle en cas de contravention à la présente politique; il en est de même pour la personne qui, par négligence, modification non approuvée ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

9. Modification et révision

La présente politique sera révisée, et modifiée au besoin, un an après son adoption initiale. Le cycle de modification et de révision sera, par la suite, à tous les trois ans.