POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Date d'entrée en vigueur : 9 décembre 2020 **Autorité approbatrice :** Conseil d'administration

Version remplacée ou amendée : s. o. **Numéro de référence :** VPS-33

PRÉAMBULE

La présente politique est adoptée conformément à l'article 7 de la Directive sur la sécurité de l'information gouvernementale. Cette directive exige des organismes publics qu'ils adoptent et mettent en œuvre une politique sur la sécurité de l'information.

PORTÉE

La présente politique s'applique à l'ensemble des membres (tel que ce terme est défini ci-après) de la communauté de l'Université Concordia (« l'Université »). Elle régit toute information (tel que ce terme est défini ci-après) détenue, recueillie, conservée, transmise ou produite par l'Université ou une tierce partie – conseil, fournisseur ou autre partenaire externe –, et ce, sur quelque support que ce soit (notamment papier ou numérique) et pour l'intégralité du cycle de vie (tel que ce terme est défini ci-après) de ladite information.

Cette politique a été élaborée dans le contexte des autres politiques et règlements de l'Université; elle coexiste avec ceux-ci, notamment avec ceux qui régissent l'utilisation de la propriété et des services de l'Université, la gouvernance des données (tel que ce terme est défini ci-après), l'utilisation d'ordinateurs, la confidentialité, la gestion des risques, la gestion des documents, les procédures disciplinaires, le droit d'auteur et la propriété intellectuelle.

OBJET

La présente politique a pour objet d'affirmer l'engagement de l'Université à assurer la sécurité de l'ensemble des données institutionnelles et des renseignements institutionnels (tel que ces termes sont définis ci-après) détenus par l'Université, et ce, conformément aux lois et règlements applicables. Plus précisément, elle vise à 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. Par ailleurs, la politique définit la structure de gouvernance ainsi que les unités ou équipes responsables d'assurer la sécurité de l'information.

DÉFINITIONS

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

« Actif » signifie tout bien matériel ou numérique qui sert à stocker, à utiliser, à transmettre ou à recevoir de l'information ou qui est lié au cycle de vie de celle-ci. Au nombre des actifs figurent notamment : applications, bases de données, serveurs, ordinateurs, portables, téléphones et cellulaires.

Les « administrateurs des données » sont les personnes qui assurent la supervision institutionnelle de l'information.

Le « cycle de vie » est l'ensemble des étapes associées à la création, à l'utilisation, à la conservation et à la destruction d'un document (tel que ce terme est défini ci-après). Au nombre de ces étapes figurent la conception, l'enregistrement, la conservation, la préservation, le transfert, la consultation, la lecture et la destruction dudit document, et ce, conformément aux règles de l'Université et aux lois applicables.

Un « document » est une information inscrite sur un médium. Délimitée et structurée en fonction du médium utilisé, cette information peut prendre la forme de mots, de sons ou d'images. Elle peut être présentée à l'aide de tout type d'écriture, y compris un système de symboles qui peut être transcrit en mots, en sons ou en images ou un autre système de symboles. Aux fins de la présente politique, une base de données dont les éléments structurants permettent de créer des documents en délimitant et en organisant l'information contenue dans ladite base de données constitue un document.

« Données institutionnelles » signifie toute représentation ou description normalisée de faits ou de chiffres pouvant être créée, recueillie, traitée, communiquée ou interprétée.

Un « entrepôt de données » est un répertoire central qui a pour objet de faciliter l'accès aux données à des fins décisionnelles. Il contient des données institutionnelles sur de nombreux sujets et provenant de sources multiples.

Le « gardien désigné » est 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.

La « gouvernance des données » est un ensemble de normes et de processus liés aux données qui sont suivis par tous les membres de la communauté et qui assurent l'exactitude, l'intégrité et l'accessibilité de l'information.

« Information » signifie aussi bien des données institutionnelles que des renseignements institutionnels ou personnels.

L'« intendant des données » est la personne responsable d'un système d'information, d'un minientrepôt de données ou d'un entrepôt de données ainsi que de l'information connexe, dont il assure la supervision.

« Membre » signifie une étudiante, un étudiant ou une personne employée à temps plein, à temps partiel ou à titre temporaire par l'Université, y compris les membres du personnel et du corps professoral, les boursières et boursiers postdoctoraux, les chercheuses et chercheurs, les membres de l'administration, les stagiaires et les bénévoles.

Un « minientrepôt de données » est un sous-ensemble d'un entrepôt de données destiné à des utilisateurs précis (tel que ce terme est défini ci-après). Il contient les données liées à un sujet particulier comme la finance, les ressources humaines ou l'effectif étudiant.

Le « Programme de sécurité de l'information » est 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.

Les « renseignements institutionnels » sont des données institutionnelles qui ont été dérivées, agrégées, traitées, organisées, structurées et présentées dans un rapport, un tableau de bord, une visualisation graphique ou des indicateurs de rendement clés, ou encore dans une base de données, un minientrepôt de données ou un entrepôt de données corollaires.

« Renseignements personnels » signifie toute information permettant d'identifier une personne.

Un « superviseur » est une personne à qui incombe la responsabilité d'encadrer directement des employées et employés de l'Université.

« Utilisateur » signifie toute personne – membre, entrepreneure ou invitée – ayant accès à l'information.

POLITIQUE

1. Les activités liées à la gestion de la sécurité de l'information doivent, d'une part, appuyer la mission de l'Université et, d'autre part, garantir la réalisation sécuritaire et ininterrompue de ladite mission par l'Université, et ce, conformément à l'ensemble des lois et normes applicables.

   La gestion de la sécurité de l'information inclut :

   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 membres de la communauté;

   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 de l'information et 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 de même qu'aux lois et normes applicables;

   f) la conception et la conservation de l'information conformément aux politiques et procédures en vigueur de l'Université, y compris, mais sans s'y limiter, le Plan de classification et de conservation des documents, la Politique sur la protection des renseignements personnels (SG-9), la Politique sur l'information confidentielle (HR-36), la Politique sur les installations informatiques (VPS-30), la Politique sur la

gouvernance des données (PRVPA-4) de même 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 membres pertinents de la communauté;

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.

Rôles et responsabilités

2. Sous l'autorité du vice-recteur aux services et au développement durable, la vice-rectrice adjointe aux systèmes d'information et chef de l'information 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.

3. Sous l'autorité de la chef de l'information, le chef de la sécurité de l'information 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.

4. Désignée par la chef de l'information et le chef de la sécurité de l'information, l'unité responsable peut rédiger des procédures, des guides, des directives ou d'autres documents relatifs aux politiques de l'Université, et ce, en vue de faciliter la mise en œuvre de la présente politique. Parmi les sujets susceptibles d'être abordés, soulignons :

   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) les procédures et lignes directrices relatives au mode PAP (« prenez vos appareils personnels »).

5. Il incombe au superviseur de s'assurer que les employées et employés ainsi que toute autre personne qu'il encadre sont informés de la présente politique et des responsabilités qui y sont définies.

6. Des comités et des équipes d'intervention – décrits à l'annexe A – ont été créés et dotés de responsabilités et de mandats spécifiques portant notamment sur :

   a) le maintien de la sécurité de l'information;

   b) la garantie de la sécurité des actifs;

   c) la réponse à toute atteinte à la protection des renseignements personnels;

   d) la prévention de la fraude; et

   e) la résolution des incidents en matière de sécurité de l'information.

Au fil du temps, ces comités et ces équipes d'intervention pourront être modifiés, étoffés ou démantelés pour répondre aux changements technologiques ou à l'évolution des besoins de l'Université.

7. Conformément à la Politique sur la gouvernance des données (PRVPA-4) et au cadre de gouvernance des données y afférent, le Service des technologies de l'information et de l'enseignement (« IITS ») et les intendants des données s'assurent que la conception, la configuration, la mise en œuvre, l'exploitation, la maintenance, la mise à niveau et la mise hors service des systèmes se déroulent selon les besoins déterminés en matière de sécurité de l'information.

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.

9. Il incombe aux administrateurs des données de s'assurer de l'exactitude de l'information, de son accessibilité à tout utilisateur autorisé et de sa classification conformément aux politiques et directives de l'Université, notamment la Politique sur la gouvernance des données (PRVPA-4) et le cadre de gouvernance des données.

10. Il incombe aux membres de l'équipe responsable de la sécurité à l'IITS et aux intendants 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 ou selon les consignes qu'imposent les autorités gouvernementales.

11. Qu'il appartienne à l'Université ou à un utilisateur, tout actif doit être confié à un gardien désigné. Il incombe à ce dernier de veiller au respect de la présente politique.

12. Il incombe notamment à l'utilisateur :

    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 – recommandée ou obligatoire – sur la sécurité de l'information;

c) d'assurer la protection de tout mot de passe ou accès que lui fournit l'IITS ou une administratrice ou un administrateur de système. Le droit d'accès est restreint à la personne qui en bénéficie, et 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.

Non-conformité

13. La non-conformité à la présente politique peut entraîner diverses sanctions, notamment 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 l'adoption de mesures disciplinaires.

Responsabilité et révision de la politique

14. La responsabilité de mettre en œuvre la présente politique et de recommander des modifications incombe au vice-recteur aux services et au développement durable.

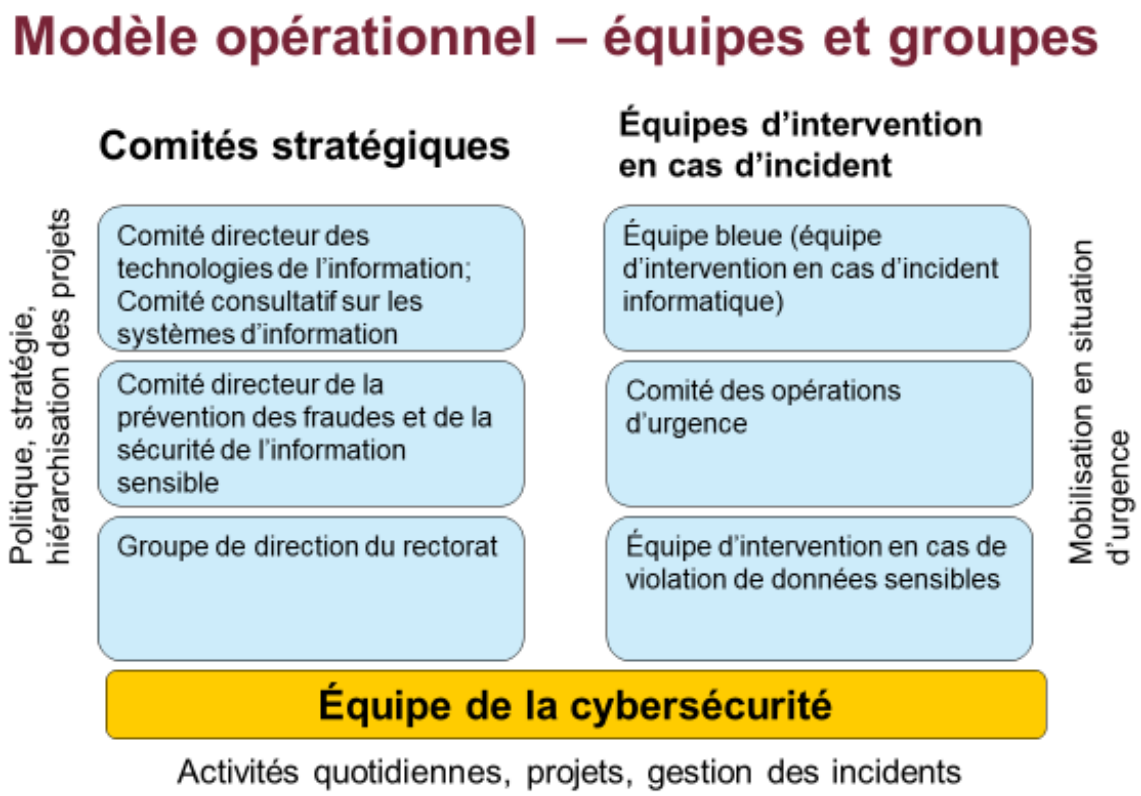
Politique approuvée par le conseil d'administration le 9 décembre 2020.

ANNEXE A

Structure de gouvernance

Il incombe à la vice-rectrice adjointe aux systèmes d'information et chef de l'information ainsi qu'au chef de la sécurité de l'information de coordonner leurs efforts à ceux que déploient, dans le cadre de diverses initiatives, les comités pertinents de l'Université.

La structure de gouvernance aux fins de la sécurité de l'information est décrite ci-après.



Comités stratégiques

1. Comité directeur des technologies de l'information

En vertu de son mandat, le comité directeur des technologies de l'information définit les orientations stratégiques relatives aux systèmes d'information et aux technologies connexes. De plus, le comité analyse la performance des technologies de l'information (« TI ») en fonction de paramètres déterminés et recommande des améliorations. Enfin, il peut être appelé à valider des demandes de financement dont la portée s'étend à l'ensemble de l'Université.

Il incombe aux membres du comité directeur des technologies de l'information :

- de revoir les initiatives stratégiques générales liées au Programme de sécurité de l'information et à l'itinéraire d'investissement;
- d'examiner les risques en matière de sécurité de l'information devant être portés à l'attention du comité de gestion des risques d'entreprise;
- de passer en revue les politiques sur les TI; et
- de faire des recommandations au groupe de direction du rectorat et au conseil d'administration sur les approbations nécessaires en matière de sécurité de l'information.

2. Comité consultatif sur les systèmes d'information

En vertu de son mandat, le comité consultatif sur les systèmes d'information surveille et optimise les résultats escomptés de l'exécution de la feuille de route des TI (dossiers de décision et projets). De même, le comité suit et maximise la gestion du cycle de vie de tout actif ainsi que la prestation des services de TI à l'utilisateur. Enfin, il fait des recommandations au comité directeur des technologies de l'information quant à ses orientations stratégiques.

Il incombe aux membres du comité consultatif sur les systèmes d'information de passer en revue les dossiers de décision et les projets inclus dans le Programme de sécurité de l'information.

3. Comité directeur de la prévention des fraudes et de la sécurité de l'information sensible

En vertu de son mandat, le comité directeur de la prévention des fraudes et de la sécurité de l'information sensible assure une gouvernance efficace en matière de sécurité de l'information à l'Université. À cette fin, il supervise le Programme de sécurité de l'information.

Il incombe aux membres de ce comité :

- de revoir le Programme de sécurité de l'information, notamment les politiques, directives, règles, procédures et pratiques exemplaires s'y rattachant; et
- d'examiner les incidents majeurs liés à la sécurité de l'information et, au besoin, les solutions proposées pour les régler.

4. Groupe de direction du rectorat

Le groupe de direction du rectorat est alerté lorsque survient un incident de cybersécurité majeur impliquant une violation de données ou une grave interruption de service. Le groupe joue un rôle stratégique dans la gestion de l'incident. Par ailleurs, il revoit les politiques et directives sur la sécurité de l'information et formule des recommandations en la matière.

Équipes d'intervention en cas d'incident

5. Équipe bleue (équipe d'intervention en cas d'incident informatique)

Groupe d'intervention, l'équipe bleue est formée pour régler un incident, participer à des exercices de table ou procéder à une simulation d'incident. Entièrement composée de spécialistes techniques, l'équipe bleue recrute ses membres auprès d'IITS et, au besoin, d'autres unités. La ou le responsable de la sécurité de l'information – ou son homologue – assure la liaison avec le chef de la sécurité de l'information de sorte que d'autres groupes, notamment le comité des opérations d'urgence, soient informés du déroulement de l'intervention de l'équipe bleue afin de régler un incident.

6. Comité des opérations d'urgence

Composé de représentantes et de représentants des principales unités de l'Université, le comité des opérations d'urgence siège à intervalles réguliers pour examiner les cas d'urgence survenus sur le campus. Le comité se réunit également pour coordonner l'intervention aux fins d'une situation critique en cours. Enfin, lorsqu'une cyberurgence est déclarée, non seulement il fait office de principal organe de coordination pour les autres unités de l'Université, mais il collabore à l'intervention pratiquée.

7. Équipe d'intervention en cas de violation de données sensibles

L'équipe d'intervention en cas de violation de données sensibles est mobilisée par le vice-recteur aux services et au développement durable (ou une personne le représentant) lorsqu'est commise une violation de données sensibles. L'équipe évalue alors la gravité et les répercussions de l'incident. Si celui-ci justifie une intervention, elle peut demander l'aide du comité des opérations d'urgence.

Équipe opérationnelle

8. Équipe de la cybersécurité

L'équipe de la cybersécurité fait appel à des analystes de la sécurité de l'information d'IITS, qui exercent des fonctions opérationnelles liées à la cybersécurité et sont responsables de projets dans ce domaine. En cas d'incident de cybersécurité, l'équipe de la cybersécurité est intégrée à l'équipe bleue.

Procédure de signalement des incidents

L'utilisateur doit signaler tout incident – établi ou présumé – au moyen de l'application de rapport d'incident offerte dans le portail MyConcordia. L'incident est alors catégorisé et traité conformément à la procédure de gestion des incidents.