# POLITIQUE DE SÉCURITÉ INFORMATIQUE

Adoptée à la séance du conseil
d'administration du 1er avril 2021

***Cette politique s'adresse à l'ensemble des utilisateurs des actifs informationnels de la Fondation de l'UQAM***

**Responsable : Direction TI**

**Table des matières**



**Les annexes**

# 1. Sommaire exécutif

La Fondation de l'UQAM (ci-après nommée Fondation) doit protéger ses données confidentielles, sensibles et à diffusion limitée, pour éviter d'impacter négativement ses donatrices et ses donateurs, prospects et autres parties prenantes et d'endommager sa réputation. La protection des données est un des besoins essentiels de la Fondation, mais tout aussi important est le fait de pouvoir facilement accéder à ces données et de travailler efficacement.

La Fondation est sous les réseaux et la sécurité de l'Université du Québec à Montréal (UQAM) et régie par le vice-rectorat aux systèmes d'information de l'UQAM. La politique numéro 47 et les règlements numéro 12 et 14 ne font pas partie de la politique de la Fondation, mais les documents sont fournis à titre de référence et les employés de la Fondation doivent les mettre en application.

La présente politique s'applique à l'ensemble des personnes employées de la Fondation et à toute personne physique ou morale appelée à utiliser les actifs informationnels de la Fondation.

Son objectif principal est de sensibiliser et d'orienter les utilisatrices et les utilisateurs quant à leurs responsabilités dans la protection des actifs informationnels.

Toute personne étant appelée à utiliser les actifs informationnels de la Fondation doit obligatoirement prendre connaissance de cette politique sur la sécurité informatique et signer l'entente de confidentialité.

La sécurité de l'information de la Fondation ainsi que les rôles et responsabilités des principaux intervenantes et intervenants en sécurité de l'information sont définis dans le document intitulé : Cadre de gestion de la sécurité informatique (CGSI) (voir Annexe 4) qui vient compléter les dispositions de la présente politique.

## 2. Préalable

La Fondation de l'UQAM (ci-après nommée Fondation) est sous les réseaux et la sécurité de l'Université du Québec à Montréal (UQAM) et régie par le vice-rectorat aux systèmes d'information de l'UQAM. À cet effet, la Fondation est assujettie à

- La politique numéro 47 - Politique sur la sécurité informatique ainsi qu'aux règlements suivants :
  - Numéro 12 - Règlement sur l'utilisation et la gestion des actifs informationnels;
  - Numéro 14 - Règlement relatif à l'emprunt d'équipement informatique et de télécommunications de l'UQAM.

La politique numéro 47 et les règlements numéro 12 et 14 ne font pas partie de la politique de la Fondation, mais les documents sont fournis à titre de référence et les employés de la Fondation doivent les mettre en application.

La présente politique sur la sécurité informatique permet de réaffirmer clairement l'intérêt des administratrices et des administrateurs de la Fondation envers la protection des actifs informationnels. Par cette politique, la Fondation fait appel à la responsabilisation personnelle de son personnel. Tous les employés doivent faire preuve dans l'exécution de leurs tâches d'un réel sens des responsabilités en matière de sécurité informatique, en vue de la protection de l'information, de l'utilisation éthique de ses actifs informationnels, de l'éducation et de la sensibilisation relatives à la sécurité informatique. Cette politique s'inscrit dans une perspective de prévention et s'appuie sur l'ensemble de ses employés qui utilisent et gèrent les actifs informationnels. Conséquemment, la politique précise les droits et obligations du personnel et de ses invitées, invités et détermine les responsabilités quant à sa mise en œuvre.

## 3. Cadre juridique

Le cadre juridique de la présente politique est constitué d'une part, par les lois canadiennes et québécoises en vigueur et, d'autre part, par les politiques, règlements et protocoles internes et externes à la Fondation, de même que par le code d'éthique et les conventions collectives en vigueur à la Fondation.

## 4. Énoncés et principes généraux

La gouvernance de la sécurité de l'information est basée sur une prise en charge engagée et imputable mettant en avant-plan l'amélioration continue, la proactivité et la reddition de comptes à tous les niveaux hiérarchiques, tout en favorisant une collaboration soutenue avec les différents intervenants et intervenantes, la sensibilisation, le partage et le renforcement des connaissances.

La sécurité informatique peut être vue comme (réf. : Politique 47 de l'UQAM) :

- Une démarche : elle se définit alors comme la poursuite active des objectifs de confidentialité, d'intégrité et de disponibilité de manière à ce que les actifs informationnels soient utilisables dans des conditions adéquates;

- Un objectif : elle se définit alors comme un objectif qui vise à maintenir les conditions adéquates pour que les actifs informationnels soient utilisables, dans le respect des exigences de confidentialité, d'intégrité et de disponibilité;

- Un résultat : elle se définit alors comme l'état des actifs informationnels qui sont utilisables dans des conditions adéquates, dans le respect des exigences de confidentialité, d'intégrité et de disponibilité.

La sécurité informatique se rapporte aux actifs informationnels qui sont l'ensemble des données et des équipements nécessaires à l'évolution de l'information tout au long de son cycle de vie, de son acquisition ou de sa création à sa destruction.

La sécurité informatique est une responsabilité organisationnelle et personnelle de sorte que l'atteinte de ces objectifs repose sur la reconnaissance et la mise en œuvre d'un ensemble de droits et responsabilités individuels qui respectent les principes directeurs suivants :

- Le respect des droits des utilisatrices et des utilisateurs tels qu'ils sont définis dans la présente politique;

- Le respect de l'autonomie du personnel dans la gestion des informations créées par le biais des activités de la Fondation;

- L'amélioration constante des mécanismes administratifs, préventifs et d'intervention pour permettre de poser les actions requises dans les situations mettant en péril la sécurité des actifs informationnels;

- La fiabilité, la qualité et le bon fonctionnement des services qui permettent à la Fondation de réaliser sa mission et ses objectifs, dans le respect des droits et libertés des personnes ainsi que des lois et règlements;

- La recherche et la mise en œuvre de moyens afin de protéger le travail des personnes en permettant une utilisation des actifs informationnels dans des conditions optimales;

- La résolution des problèmes de sécurité informatique par une approche « proactive » et préventive plutôt que par une approche réactive;

- La sensibilisation des utilisatrices et des utilisateurs des actifs informationnels de la Fondation, en mettant les moyens nécessaires à leur disposition, à l'importance d'assumer les responsabilités préconisées par la Politique sur la sécurité informatique, et ce, considérant qu'ils sont les principaux artisans de la mise en application efficace d'une telle politique à la Fondation.

## 5. Objectifs

La Fondation doit protéger ses données confidentielles, sensibles et à diffusion limitée, pour éviter d'impacter négativement ses donatrices et ses donateurs, prospects et autres parties prenantes et d'endommager sa réputation. La protection des données est un des besoins essentiels de la Fondation, mais tout aussi important est le fait de pouvoir facilement accéder à ces données et de travailler efficacement.

Son objectif principal est de sensibiliser et orienter les utilisateurs quant à ses responsabilités dans la protection des actifs informationnels. Cette politique met en avant les conditions requises pour la prévention de la fuite des données et, plus spécifiquement :

- Le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs aux prospects, donatrices et donateurs, au personnel de la Fondation et autres parties prenantes;

- La conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales et, plus particulièrement, permettre de respecter les prescriptions du cadre normatif de la sécurité de l'information quant aux renseignements nominatifs et aux informations à caractère confidentiel transmis ou conservés à l'aide d'actifs informationnels;

- La disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité à l'égard de l'ensemble des activités d'accès, d'utilisation, de collecte, d'enregistrement, de traitement, de conservation, de diffusion et de transmission des actifs informationnels de la Fondation, de même que la continuité des services;

- La sécurité de l'information en regard de l'utilisation des réseaux informatiques et de l'Internet notamment des médias sociaux;

- Une conduite rigoureuse de tout utilisatrice, utilisateur face aux actifs informationnels sensibles pour les fins de statistiques;

- Le respect du code d'éthique (voir Annexe 2);

- Préserver l'image et la crédibilité de la Fondation;

- Sensibiliser tout utilisatrice, utilisateur sur l'exercice de ses libertés et de ses droits fondamentaux dans le respect de ceux d'autrui et du bien-être général;

- Sensibiliser tout utilisateur aux problématiques pouvant se poser en raison de l'utilisation de moyens de réseautage individuel;

- Mettre en œuvre des mesures préventives et dissuasives pour assurer un environnement respectueux des libertés de moyens de réseautage virtuel.

Tous les employés de la Fondation doivent connaître cette politique et agir conformément à leurs responsabilités, telles que définies dans cette politique.

## 6. Champ d'application

### 6.1 Les personnes visées :

La présente politique s'applique à l'ensemble des personnes employées de la Fondation. Elle touche également toute personne physique ou morale appelée à utiliser les actifs informationnels de la Fondation.

### 6.2 Les actifs et services visés :

- Les actifs informationnels de la Fondation détenus dans l'exercice de sa mission, que sa conservation soit assurée par la Fondation ou par un tiers;
- Les contrats et les ententes de services en lien avec des actifs informationnels;
- Toute information traitée électroniquement et/ou conservée sur papier.

## 7. Structure fonctionnelle

Tous les utilisateurs, utilisatrices des actifs informationnels de la Fondation ont des droits quant à la sécurité informatique. Ces droits varient en fonction du ou des rôles des utilisateurs dans l'utilisation et dans la gestion des actifs informationnels appartenant à la Fondation. Ceux-ci, dans le cadre de la gestion des actifs informationnels, ont donc le devoir de respecter ces droits dans toutes les décisions et actions entreprises.

Les utilisatrices, utilisateurs des actifs informationnels de la Fondation ont également des responsabilités à l'égard de la sécurité informatique. Le respect de ses responsabilités permettra, selon son rôle, de contribuer à différents degrés à la sécurité des actifs informationnels.

Tous les utilisateurs et utilisatrices des actifs informationnels de la Fondation sont responsables d'une saine utilisation des actifs informationnels. L'annexe 4 : Cadre de gestion de la sécurité informatique de la présente politique sur la sécurité informatique présente de façon détaillée les rôles et responsabilités des utilisatrices, utilisateurs des actifs informationnels de la Fondation.

## 8. Droit de regard

La Fondation se réserve un droit de regard sur tout usage des actifs informationnels de l'établissement.

## 9. Rôle et responsabilités

La structure fonctionnelle de la sécurité de l'information de la Fondation ainsi que les rôles et responsabilités des principaux intervenants et intervenantes en sécurité de l'information sont définis dans le document intitulé : Cadre de gestion de la sécurité informatique (CGSI) (voir Annexe 4) qui vient compléter les dispositions de la présente politique.

Le directeur des technologies de l'information et/ou le responsable des technologies de l'information, délégué par le directeur général, est responsable de l'application de la politique de sécurité de l'information.

## 10. Sanctions

Lorsqu'un utilisateur, une utilisatrice ou une organisation contrevient ou déroge à la présente politique ou aux directives en découlant, il s'expose selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste.

## 11. Dispositions finales

La présente politique entre en vigueur à la date de son approbation par le conseil d'administration de la Fondation. Cette politique est réévaluée minimalement aux trois ans afin d'intégrer les nouveaux besoins, les nouvelles pratiques, les nouvelles menaces et les nouveaux risques encourus.

# Annexe 1 : Définitions

**Actif informationnel**

Tout équipement relié ou non au réseau, logiciel, système, donnée ou information utilisés pour l'hébergement, le traitement, la diffusion et l'échange d'information. Les actifs informationnels de la Fondation couvrent les équipements, logiciels, systèmes, données ou informations qui lui appartiennent et ceux qui utilisent ou hébergent des actifs dont la Fondation et l'Université sont propriétaire, fiduciaire ou dépositaire.

**Authentification**

Une caractéristique exclusive, une information unique et confidentielle ou un objet unique détenu par une personne ou par toute autre entité, permettant de vérifier l'identité de cette personne ou entité. Une signature manuscrite, une empreinte digitale, un mot de passe ou un numéro d'identification personnel sont des exemples d'authentifiant.

**Cadre normatif de la sécurité de l'information**

Ensemble de textes encadrant la sécurité de l'information, incluant la Politique de l'Université du Québec à Montréal (UQAM) de sécurité de l'information, le Cadre de gestion de la sécurité de l'information (CGSI) de la Fondation, les règles particulières sur la sécurité organisationnelle de l'UQAM, les guides et procédures qui s'y rattachent.

**Confidentialité**

Une exigence en vertu de laquelle une information est divulguée, traitée et mise à la disposition des seules personnes ou entités autorisées, selon les modalités établies.

**Disponibilité**

Une exigence en vertu de laquelle la propriété d'un actif informationnel est accessible et utilisable par une personne ou par une entité, dans les conditions autorisées.

**Intégrité**

Une exigence se rapportant aux données ou aux systèmes. L'intégrité des données est une exigence qui veut que l'information et les programmes ne soient modifiés que d'une manière déterminée et autorisée, tandis que l'intégrité des systèmes est une exigence qui veut qu'un système remplisse les tâches auxquelles il est destiné, libre de toute manipulation non autorisée, qu'elle soit délibérée ou commise par inadvertance.

**Irrévocabilité**

Propriété d'un acte d'être définitif et qui est clairement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

**Invitée, invité**

Ensemble des individus utilisant les actifs informationnels de la Fondation sur une base régulière ou ponctuelle et n'étant pas assujetti à un lien d'emploi ou à un lien contractuel formel avec la Fondation.

**Médias sociaux**

Toute forme d'application, plateforme et média virtuel en ligne visant l'interaction sociale la collaboration, la création et le partage de contenu. Les médias sociaux sur Internet comprennent notamment :

- Les sites sociaux de réseautage.
- Les sites de partage de vidéos ou de photographies.
- Les sites de microblogage.

- Les blogues.
- Les forums de discussion.
- Les encyclopédies en ligne.

**Responsabilité et imputabilité**

Le plus haut dirigeant d'un organisme est l'ultime responsable de la sécurité de l'information relevant de son autorité. À ce titre, il prend les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité de l'information de son organisme.

- Toute personne, autorisée à avoir accès aux actifs informationnels de la Fondation assume des responsabilités particulières en matière de sécurité de l'information, notamment en terme de protection de l'information et répond de ses actions auprès du plus haut dirigeant de la Fondation.

**Sensibilisation et formation**

Un programme continu de sensibilisation et de formation à la sécurité de l'information doit être mis en place. Des activités de sensibilisation et de formation des utilisatrices et des utilisateurs à la sécurité de l'information, aux conséquences d'une atteinte à la sécurité de l'information, ainsi qu'à leurs rôles et leurs obligations en cette matière doivent être effectuées.

**Utilisatrice, utilisateur**

L'ensemble des personnes employées par la Fondation ainsi que toute personne physique ou morale appelée à utiliser les actifs informationnels de la Fondation ou à traiter l'information appartenant à la Fondation.

## 1 PRINCIPES

1.1 Ce code d'éthique a pour but d'assurer les donatrices et les donateurs que l'organisation qu'ils ont choisie soutient une cause philanthropique en accord avec des objectifs économiques, sociaux, et culturels conformes à l'éthique. Ainsi, en aucun temps, ces objectifs ne contreviennent aux droits de la personne, tant sur le plan individuel que collectif. Ils sont en accord avec l'écologie et des principes de développement durable. Ils poursuivent des buts pacifiques et n'encouragent aucune cause qui risque d'engendrer des conflits.

En effet, la Fondation de l'UQAM a pour mandat de recueillir des fonds pour l'Université du Québec et ses étudiants. Les dons représentent une contribution à la formation, à l'enseignement et la recherche/création ainsi qu'aux services à la collectivité et ils correspondent en tous points aux objectifs énoncés précédemment.

1.2 Le code d'éthique vise à ce que les membres du personnel de la Fondation avec lesquels les donateurs transigent respectent leurs projets de dons, aient des communications ainsi qu'un mode d'action transparents et les conseillent de manière complète et objective. De plus, le code doit servir les intentions, la liberté de choix et la vie privée des donateurs.

1.3 Les membres du personnel de la Fondation doivent de plus respecter la mission et les objectifs poursuivis par la Fondation de l'UQAM et l'Université du Québec à Montréal. Les dons reçus doivent avoir un lien direct avec les objectifs universitaires mentionnés précédemment.

1.4 Les membres du Conseil d'administration ainsi que les bénévoles de la Fondation sont tenus d'adhérer à l'esprit de ce Code, tant dans la gestion de l'organisme que dans leurs contacts avec des donateurs.

1.5 Tous les membres du personnel, du Conseil d'administration ainsi que les bénévoles et invités de la Fondation ont l'obligation de prendre connaissance de la politique sur la sécurité informatique de la Fondation ainsi que la politique sur la sécurité informatique en vigueur à l'UQAM et des règlements s'y afférant.

## 2 NORMES D'ÉTHIQUE PROFESSIONNELLE

### 2.1 La Fondation

2.1.1 La Fondation de l'UQAM et les membres de son personnel adoptent des pratiques et des procédures qui respectent les principes de saine gestion et les principes comptables généralement reconnus. Les rapports annuels sont disponibles pour consultation et sont remis aux donatrices et donateurs qui en font la demande.

2.1.2 Les dossiers des donatrices et des donateurs, les renseignements personnels et financiers qui constituent les dossiers, de même que les conversations avec les membres du personnel, font l'objet de la confidentialité la plus stricte. Cette même mesure s'applique aussi aux donateurs potentiels.

2.1.3 La Fondation de l'UQAM s'engage à ce que les dossiers des donateurs ainsi que les renseignements qui y sont contenus demeurent sa propriété exclusive et ne puissent être transférés, sans le consentement explicite des donateurs.

2.1.4 La Fondation de l'UQAM s'engage à respecter l'anonymat des donateurs qui en font la demande.

2.1.5 La Fondation de l'UQAM s'engage à respecter le calendrier et le mode de sollicitation choisis par les donateurs.

2.1.6 Les membres du personnel de la Fondation étant rémunérés, en aucun temps, ceux-ci ne doivent recevoir en sus, des honoraires, des primes, des commissions ou d'autres avantages financiers de la part de donateurs ou des intermédiaires qui agissent dans des dossiers de dons pour le compte de leur clientèle.

2.1.7 La Fondation et les membres de son personnel veillent à ce que les dons reçus servent aux fins auxquelles les donateurs les ont destinés et ce, de façon continue.

2.1.8 La gestion des fonds de dotation pour le compte des donateurs est dédiée aux objectifs poursuivis par ces personnes ainsi qu'aux priorités confiées par l'UQAM à la Fondation. Des rapports annuels sont fournis aux donateurs ou à leurs représentants. Aucun changement n'est effectué à l'attribution de ces fonds sans le consentement explicite de ces personnes.

2.1.9 Toute situation irrégulière doit être portée à l'attention du directeur général de la Fondation qui a la responsabilité d'agir et le cas échéant, au Conseil d'administration qui verra à prendre les correctifs appropriés, en protégeant l'anonymat de la personne qui a effectué le signalement et en s'assurant que cette dernière ne subira aucune représailles.

## 2.2 Les membres du personnel

2.2.1 Le rôle premier des membres du personnel de la Fondation de l'UQAM est de répondre aux désirs véritables des donatrices et des donateurs de soutenir l'UQAM et ses étudiants.

2.2.2 Les membres du personnel de la Fondation doivent agir dans leurs communications et leurs ententes avec les donateurs avec compétence, franchise, intégrité et équité.

2.2.3 Le travail des membres du personnel de la Fondation est d'éclairer les donateurs, de les soutenir et d'assurer la réalisation de leurs objectifs philanthropiques. De plus, ils voient à ce que les dons puissent être traités dans les meilleures conditions possibles, tant pour les donateurs que pour la Fondation de l'UQAM.

2.2.4 Pour ce faire, ces personnes ont la responsabilité de transmettre aux donateurs les renseignements utiles à la compréhension de tous les aspects relatifs à leurs dons, incluant l'impact fiscal. En cas d'ignorance d'un élément technique, elles font la recherche et leur répondent de façon complète et précise. Si requis, elles doivent faire connaître explicitement leur rôle au sein de la Fondation de l'UQAM. Elles ont le devoir d'informer les donateurs de leurs domaines d'expertise et de leurs limites. Elles peuvent recourir aux services d'experts en cas de besoin.

2.2.5 Les membres du personnel de la Fondation ont le devoir d'encourager les donateurs à consulter leurs conseillers personnels ou des professionnels indépendants dans le cas de transactions de dons significatifs et plus complexes. Les représentants de la Fondation collaborent avec ceux-ci dans le même esprit qu'avec les donateurs.

2.2.6 Les membres du personnel agissent aussi comme des représentants de l'établissement pour lequel la Fondation a été créée; à ce titre, ils s'assurent que les dons offerts par les donateurs soient conformes aux objectifs poursuivis par l'UQAM. En tout temps, ils doivent tenir compte tant des intérêts des donateurs que des objectifs institutionnels.

2.2.7 À titre de représentants de la Fondation et de l'UQAM, les membres du personnel agissent comme des fiduciaires pour le traitement des dossiers et des renseignements qui leur sont transmis. En aucun temps, ces renseignements ne doivent être utilisés à des fins personnelles.

2.2.8 Ces personnes ont la responsabilité de maintenir un haut niveau de compétence professionnelle et de parfaire leurs connaissances sur une base régulière.

2.2.9 À moins de circonstances exceptionnelles, les membres du personnel de la Fondation de l'UQAM n'acceptent pas d'agir pour le compte des donateurs (exemple: exécuteurs testamentaires) de manière à éviter tout conflit d'intérêt. Le cas échéant, la charge est rattachée à la fonction plutôt qu'à la personne qui l'occupe.

2.2.10 En aucun temps, ils ne doivent tirer d'avantages pécuniaires de transactions reliées à des dons ou à des relations établies avec des donatrices et des donateurs dans le cadre de leurs fonctions.



J'ai pris connaissance du code d'éthique en vigueur à la Fondation de l'UQAM, de la politique sur la sécurité informatique de la Fondation ainsi que celle de l'UQAM (politique #47) et des règlements en vigueur à l'UQAM (#12 et #14) et je m'engage à y adhérer sans réserve.

Signé ce _____e jour de _____

Par _____

«Prénom» «Nom»

**EXPOSÉ DES MOTIFS**

La Fondation de l'UQAM tient à jour un système d'information et des dossiers contenant des renseignements personnels et confidentiels sur ses donateurs. Ces renseignements sont utilisés dans le but :

a) d'établir et entretenir la communication et le contact avec les diplômés et amis de l'Université du Québec à Montréal;

b) d'appuyer les besoins et les attentes de l'Université en matière de collecte de fonds;

c) d'appuyer les activités courantes de l'Université du Québec à Montréal en offrant de l'aide au niveau des programmes, de la communication et des événements qui rassemblent les anciens, les donateurs et les amis.

Je, soussigné(e), m'engage en ma qualité de membre du personnel de la Fondation de l'Université du Québec à Montréal à :

a) garder confidentiels, à ne pas photocopier ni faire photocopier et à ne pas divulguer les informations et documents qui me seront communiqués au cours de mon mandat, sauf aux employés de la Fondation et sauf dans le cas d'une permission écrite de la direction générale de la Fondation.

b) ne pas utiliser ou copier les données dans un environnement autre que dans le contexte du travail qui m'est confié à la Fondation.

c) ne conserver aucun document numérique sur le disque local d'un ordinateur personnel ou sur un espace de stockage autre que ceux offerts par la Fondation par le biais de l'UQAM.

d) ne partager aucun document sur TEAMS ou autres plateformes de partage de document si je ne peux en assurer la confidentialité des informations.

Cet engagement est permanent et il demeure en vigueur même après la fin de mon mandat.

Signé ce _____e jour de _____20___

Par : _____
Nom de l'employé

**Annexe 4**

# Cadre de gestion de la sécurité informatique

# Fondation de l'UQAM

**Responsable : Direction TI**

**1er avril 2021**

## 1. PRÉAMBULE

La Fondation de l'Université du Québec à Montréal (ci-après nommée : La Fondation) reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. La Fondation reconnaît détenir, en outre, des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative ou économique. Le Cadre de gestion de la sécurité de l'information (CGSI) décrit les rôles et responsabilités en matière de sécurité de l'information.

## 2. OBJECTIFS

Le CGSI complète les dispositions de la politique de la sécurité de l'information de la Fondation par la mise en place d'une structure fonctionnelle de la sécurité de l'information et par la définition des rôles et responsabilités en la matière. Les rôles et responsabilités définis dans le CGSI concernent l'approbation, la mise en place, la coordination, le développement, le suivi et

l'évaluation de la sécurité de l'information à la Fondation, en tenant compte des exigences du cadre légal et administratif applicable et des principes généraux de la politique de sécurité de l'information de l'Université du Québec à Montréal.

# 3. RÔLES ET RESPONSABILITÉS

## 3.1 . Le conseil d'administration (CA) de la Fondation

- Adopte la présente politique établie par la Fondation en matière de sécurité de l'information, s'assure de sa mise en œuvre et du suivi de son application;
- Reçoit et entérine annuellement ou au besoin le Bilan de sécurité de l'information de la Fondation.

## 3.2 La directrice générale, le directeur général :

- S'assure que les valeurs et orientations en matière de sécurité soient partagées à toute personne de la Fondation de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilisent un actif informationnel sous la responsabilité de la Fondation ou y ont accès.
- S'assure du respect des lois et des règles de sécurité de l'information s'appliquant à L'UQAM;
- S'assure qu'un bilan annuel de sécurité soit présenté au CA ;
- Nomme le responsable de la sécurité de l'information et s'assure de lui octroyer les pouvoirs et ressources nécessaires à la réalisation de ses tâches et responsabilités;
- Approuve le CGSI de la Fondation;
- S'assure de la mise en œuvre de la politique de sécurité de l'information adoptée par le CA et des rôles et responsabilités du Cadre de gestion de la sécurité de la Fondation;
- S'assure de la gestion adéquate des risques de sécurité de l'information en lien avec son contexte organisationnel.

## 3.3 Le directeur et ou le responsable des technologies de l'information :

- Veille à l'élaboration, au maintien et à l'application de la politique sur la sécurité de l'information;

- Est responsable de l'élaboration du Plan directeur de sécurité et assure sa mise en œuvre et son suivi;
- Planifie les activités nécessaires à la mise en place de la sécurité de l'information au sein de la Fondation;
- S'assure de l'élaboration et de la mise en œuvre d'un programme formel de formation et de sensibilisation en matière de sécurité de l'information;
- S'assure de la mise en place du registre d'autorité de la sécurité de l'information, dans lequel sont notamment consignés les noms des détentrices et détenteurs de l'information et les systèmes d'information qui leur sont assignés;
- S'assure de la mise en œuvre d'un processus de gestion des incidents de sécurité de l'information à la Fondation;
- Veille à la mise en œuvre de toute recommandation jugée pertinente découlant d'une vérification ou d'un audit de sécurité;
- S'assure de la production d'un bilan annuel ou, au besoin, d'un plan d'action triennal de la sécurité de l'information pour la Fondation, les valide et les transmet à son dirigeant;
- Agit à titre de porte-parole auprès du CA de la Fondation en informant les différents intervenants et intervenantes en sécurité de l'information, des orientations et des priorités d'intervention et s'assure de leur mise en œuvre ;
- S'assure de l'encadrement de la sécurité de l'information au sein de la Fondation, veille à l'application de la politique et du CGSI de la Fondation et s'assure du respect par la Fondation, des règles particulières publiées par l'UQAM en matière de sécurité de l'information ;
- Dirige la coordination et la cohérence des activités de sécurité de l'information menées à la Fondation.

### 3.4 Les gestionnaires :

- Sont responsables de leur actif et en suivent l'état de la sécurité. Il s'assure que les mesures de sécurité appropriées soient élaborées et suivies dans leur secteur respectif;
- Informent le directeur des technologies de l'information ou le responsable des TI de l'existence de leur actif et de sa sensibilité;
- S'assurent que tout le personnel est informé de leurs obligations découlant de la présente politique;
- Informent leur personnel des normes, directives et procédures de sécurité en vigueur;
- S'impliquent dans l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques, la prise en charge des risques résiduels, la relève et la continuité du processus d'affaires associé à l'actif;
- Déterminent les règles d'accès aux actifs dont ils assument la responsabilité;

- Mettent en place les moyens facilitant la formation et la sensibilisation des utilisatrices et des utilisateurs quant à l'importance de la sécurité de l'information;
- S'assurent que les moyens de sécurité soient utilisés de façon à protéger l'information utilisée par leur personnel;
- Communiquent à la directrice, au directeur et / ou au responsable des technologies de l'information tout problème de sécurité qu'ils jugent important et participent à l'application de la procédure de gestion des incidents.

### 3.5 Le personnel du secteur des technologies de l'information:

- Est responsable de leur actif et en suivent l'état de la sécurité. Il s'assure que les mesures de sécurité appropriées soient élaborées et suivies;
- Informe le directeur des technologies de l'information ou responsable des TI de l'existence de leur actif et de sa sensibilité;
- S'implique dans l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques, la prise en charge des risques résiduels, la relève et la continuité du processus d'affaires associé à l'actif;
- Détermine les règles d'accès aux actifs dont ils assument la responsabilité;
- Définisse les limites raisonnables de la disponibilité, de l'intégrité et de la confidentialité pour leurs actifs, en conformité avec le Cadre normatif de la sécurité de l'information de l'UQAM.
- Fixe les moyens facilitant la formation et la sensibilisation des utilisatrices, des utilisateurs quant à l'importance de la sécurité de l'information;

### 3.6 Les pilotes de systèmes :

- Ont la responsabilité de s'assurer du fonctionnement sécuritaire d'un actif informationnel dès sa mise en exploitation, de contrôler et d'autoriser l'accès logique à tout actif informationnel dont ils ont la responsabilité d'utilisation;

- Informent les utilisatrices et utilisateurs de leurs obligations face à l'utilisation des systèmes d'information dont ils sont responsables lors de l'attribution des accès.

### 3.7 Le personnel utilisateur :

- Est responsable de respecter la présente politique, normes, directives et procédures en vigueur qui en découlent et d'informer la directrice, le directeur des technologies de l'information de toute violation des mesures de sécurité dont ils pourraient être témoins ou de toutes anomalies décelées pouvant nuire à la sécurité des actifs informationnels;
- Signe une déclaration d'allégeance et d'engagement à la confidentialité (annexe 3);
- Participe au programme de sensibilisation et de formation sur les actifs informationnels de la Fondation.

### 3.8 Les invitées, invités

- S'engagent à respecter la présente politique, les normes institutionnelles de sécurité informatique ainsi que les règlements en matière d'utilisation des actifs informationnels.
- S'engagent notamment à assumer les responsabilités applicables à l'accès accordé dans le cadre de leur visite à la Fondation.

Dans le cas où le besoin d'accès aux services dépasse les accès généralement accordés aux invitées, invités, il est possible de faire une demande d'autorisation d'accès afin d'obtenir la connexion requise.

## 4. Sécurité

Les applications sont attribuées en fonction des tâches et des besoins de chaque employé de la Fondation. Il faut noter que le code d'accès aux réseaux de l'université assure l'accès à des ressources de base tel que la suite Office, mais il ne donne pas l'accès aux applications propres à la Fondation. Dans cette perspective, le service des technologies de l'information (TI) de la Fondation et la direction s'assurent que chaque utilisatrice, utilisateur ait accès aux ressources nécessaires pour exercer ses fonctions.

NB : Une entente signée entre le Bureau des diplômés et la Fondation permet un partage de la base de données (Raiser's Edge) entre les deux entités. Les utilisatrices, utilisateurs du Bureau de diplômés de l'UQAM n'ont accès qu'aux données des diplômés. Aucune information sur les dons n'est fournie.