

HEC MONTRÉAL

Politique de sécurité de l'information

**Adoptée par le Conseil d'administration
le 10 novembre 2011**



Table des matières

PRÉAMBULE

1. GÉNÉRALITÉS	3
2. RÔLES ET RESPONSABILITÉS.....	4
3. DÉFINITIONS.....	8
4. CADRE LÉGISLATIF ET RÉGLEMENTAIRE	9

Préambule

Les opérations de HEC Montréal dépendent en grande partie de l'information qui est traitée, produite et communiquée. Cette information est très vaste et peut exister sur support papier ou technologique. Elle comprend, entre autres, les renseignements personnels des étudiants et des membres du personnel, la propriété intellectuelle produite par les enseignants et les chercheurs, ainsi que la documentation interne stratégique et administrative.

Comme toute autre institution d'enseignement supérieur, HEC Montréal fait face à une multitude de menaces pouvant porter atteinte à la confidentialité, l'intégrité et la disponibilité de son information. Ces menaces, dont la nature est en constante évolution, comprennent, entre autres, le vol d'identité et d'information confidentielle, la fraude, l'espionnage industriel et le vol de propriété intellectuelle, l'utilisation, la divulgation et la destruction d'information, les défaillances techniques, les événements naturels et l'erreur humaine.

Par ailleurs, l'École est soumise à plusieurs exigences légales, réglementaires, contractuelles ou découlant de ses propres politiques touchant à la sécurité de l'information. Le respect de ces exigences et le lien de confiance qui existe envers l'École de la part des membres du personnel, des enseignants, des étudiants et du public en général sont essentiels au maintien de sa réputation.

Il est donc impératif que l'École protège adéquatement l'information qu'elle possède ou qui lui est confiée.

1. Généralités

Objectif

Cette politique constitue un des éléments clés permettant d'assurer la réalisation de la mission et des objectifs d'affaires de l'École, de maintenir sa réputation et de se conformer aux exigences légales, réglementaires et contractuelles applicables.

L'objectif principal de cette politique est de communiquer la détermination et l'engagement de l'École de gérer avec efficacité et efficience les risques à la sécurité de l'information. L'approche préconisée vise l'identification des intervenants et la définition de leurs rôles, la sensibilisation des utilisateurs aux risques et la conception et l'implantation de mesures qui assurent efficacement la sécurité des actifs informationnels.

Portée

La sécurité de l'information est l'affaire de tous. Cette politique s'applique à tous les utilisateurs des ressources informationnelles de l'École qui incluent, entre autres, les membres de la haute direction, les gestionnaires, les membres du personnel, les enseignants, les étudiants et les assistants de recherche, ainsi que les sous-traitants, fournisseurs et partenaires de HEC Montréal.

Cette politique s'applique à toute l'information que détient HEC Montréal dans l'exercice de ses fonctions ou dont elle a la garde, durant tout son cycle de vie, peu importe sa forme, son support et son emplacement.

Principes directeurs

Les principes qui orientent la démarche de l'École, la répartition des responsabilités et la nature des actions et des moyens mis de l'avant sont les suivants :

a. Imputabilité

Chaque direction ou service administratif est imputable de la gestion des risques à la sécurité de l'information en sa qualité de propriétaire de l'information. Cette imputabilité s'applique aux actifs informationnels, aux processus et aux systèmes sous sa responsabilité ou son contrôle, incluant ceux délégués à un tiers.

b. Proportionnalité

Des mesures raisonnables sont mises en place pour garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels, à un coût proportionnel à la sensibilité de l'information et aux risques sous-jacents, différents types d'information pouvant nécessiter des niveaux de protection différents.

D'autre part, les mesures mises en place pour protéger les actifs informationnels ne doivent pas nuire à la mission de l'École.

c. Conformité

La gestion des risques à la sécurité de l'information est faite en conformité avec les exigences légales, réglementaires et contractuelles applicables ainsi qu'avec les politiques et règlements de HEC Montréal.

d. Sensibilisation

Des mesures adéquates sont mise en place pour sensibiliser et faire participer activement tous les utilisateurs et intervenants à la protection de l'actif informationnel de l'École et favoriser une utilisation responsable des ressources.

2. Rôles et responsabilités

La présente politique et son application relèvent de différents intervenants à qui les mandats suivants sont attribués :

Conseil d'administration

- Approuve la politique ainsi que ses mises à jour;
- Supervise le processus de gestion des risques à la sécurité de l'information, par l'intermédiaire du Comité d'audit.

Comité d'audit

- Recommande au Conseil d'administration l'adoption de la politique ainsi que ses mises à jour;
- Supervise le processus de gestion des risques à la sécurité de l'information et l'application de la politique;
- Rend compte, au besoin, au Conseil d'administration.

Direction

- Valide la politique ainsi que ses mises à jour et recommande au comité d'audit son adoption par le Conseil d'administration;
- S'assure de l'application de la politique par les gestionnaires de HEC Montréal;
- S'assure que le programme de sécurité de l'information dispose des ressources financières et logistiques appropriées.

Conseiller à la sécurité de l'information

- Élabore la politique et ses mises à jour et coordonne sa mise en œuvre;
- Assiste les directions et les services administratifs dans l'évaluation et la gestion des risques à la sécurité de l'information, tout en leur permettant d'atteindre leurs objectifs d'affaires;
- Identifie et maintient la liste des propriétaires d'information;
- Fournit des directives, propose des solutions, coordonne leur mise en place et facilite la conformité en matière de sécurité de l'information;
- Communique à la communauté HEC leurs responsabilités concernant la sécurité de l'information;
- Élabore et met en œuvre le programme de sensibilisation à la sécurité de l'information pour les membres du personnel, en collaboration avec la direction des technologies de l'information et la gestion des connaissances et de la direction des ressources humaines;
- Maintient le registre des incidents à la sécurité de l'information et gère le processus hiérarchique et de résolution de problème dans ce domaine;
- Effectue le suivi des observations et des recommandations des vérificateurs en matière de sécurité de l'information;
- Intervient en tout temps pour confirmer l'existence ou le bon fonctionnement d'une mesure de sécurité ou pour émettre des recommandations, si les actifs informationnels de HEC Montréal sont jugés à risque;
- Communique les risques à la sécurité de l'information et rend compte de l'application de la présente politique au Comité de direction;
- Prend les actions appropriées suite à un incident majeur touchant à la sécurité de l'information, en collaboration avec la direction des technologies de l'information et gestion des connaissances;

Direction ou service administratif

- Évalue et gère les risques à la sécurité de l'information;
- S'assure que des mesures de protection adéquates et raisonnables sont mises en place;
- Assigne un propriétaire de l'information pour chaque processus d'affaire, activité importante, système ou catégorie d'information;
- Conserve la responsabilité de la protection de l'information lorsque cette dernière est déléguée à un tiers;
- Gère les contrats et la relation avec les fournisseurs pour tout aspect touchant à la sécurité de l'information, en collaboration avec le conseiller à la sécurité de l'information et la direction des approvisionnements ;
- Maintient la classification de sécurité de l'information;
- Informe et sensibilise toute personne sous sa responsabilité de l'importance de la sécurité de l'information et de l'existence de la présente politique et des autres directives applicables;
- Communique au conseiller à la sécurité de l'information tout risque important à la sécurité de l'information.

Propriétaire de l'information

- Agit en tant que responsable désigné par son unité administrative en appliquant les dispositions de la présente politique;

- Effectue la classification de sécurité de l'information selon les directives et standards de HEC Montréal, et communique les résultats au conseiller à la sécurité de l'information;
- Établit et révisé périodiquement les profils d'accès des utilisateurs et les communique aux intervenants pertinents;
- Identifie les exigences légales, réglementaires et contractuelles applicables à la sécurité de l'information en collaboration avec le service des affaires juridiques et le conseiller à la sécurité de l'information;
- Effectue l'évaluation des risques à la sécurité de l'information et communique les résultats au conseiller à la sécurité de l'information;
- Accepte, au nom de son unité administrative, les risques résiduels à la sécurité de l'information;

Direction des ressources humaines

- Vérifie, au besoin, les antécédents des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information;
- S'assure que les responsabilités des intervenants concernant la sécurité de l'information et le respect de la présente politique sont inscrites dans les descriptions de tâches des membres du personnel;
- Appuie le conseiller en sécurité de l'information lors de l'élaboration et de la mise en œuvre du programme de sensibilisation à la sécurité de l'information pour les membres du personnel;
- Intervient auprès des membres du personnel concernés en cas d'atteinte à la sécurité de l'information, en collaboration avec le conseiller à la sécurité de l'information et les autres intervenants;
- Prend action, fait le suivi et impose les sanctions appropriées lors de violation des politiques, règlements et code de conduite touchant à la sécurité de l'information, en collaboration avec le supérieur immédiat;
- Informe les intervenants concernés d'une embauche, d'un changement de fonctions, du transfert et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels.

Affaires juridiques

Les mesures mises de l'avant prévoient que le responsable des affaires juridiques:

- Interprète les lois et règlements pouvant avoir un impact sur la sécurité de l'information;
- Communique les exigences légales, réglementaires et contractuelles applicables au conseiller à la sécurité de l'information, au propriétaire de l'information et aux autres intervenants, au besoin;
- Valide les clauses contractuelles touchant à la sécurité de l'information, en collaboration avec le conseiller à la sécurité de l'information;
- S'assure que des mesures contractuelles adéquates sont prévues afin de protéger l'information et de se conformer à la présente politique, en collaboration avec la direction des approvisionnements et le conseiller à la sécurité de l'information;
- Élabore et diffuse, en collaboration avec le conseiller à la sécurité de l'information et les autres intervenants, les politiques concernant la vie privée, la protection des renseignements personnels et la sécurité de l'information.

Service de la gestion des documents et des archives

- Assiste les unités administratives dans l'identification et la mise en œuvre de modes sécuritaires de gestion de l'information;
- Met en place les mesures de sécurité adéquates et raisonnables pour la gestion des documents semi-actifs, des archives de HEC Montréal et de certaines archives privées, en conformité avec la présente politique;
- Assure la destruction sécuritaire de l'information sous sa garde, lorsque requis par la finalité de l'information ou à la demande des directions et services administratifs.

Service de sécurité

- Contrôle l'accès physique aux locaux de l'École;
- Gère les moyens d'accès physique (clefs, cartes magnétiques, codes d'accès, biométrie, etc.) aux locaux à accès restreint (salles informatiques, archives institutionnelles, entreposage, etc.);
- Contrôle la circulation des équipements sortant des locaux de l'École;
- Collabore avec le conseiller à la sécurité de l'information et les autres intervenants aux activités de sensibilisation à la sécurité de l'information.

Direction des technologies de l'information et gestion des connaissances

- Développe et met en œuvre les directives, processus, standards et procédures touchant à la sécurité des actifs informationnels, touchant notamment à la gestion des accès, la gestion des incidents et l'intégrité de l'information;
- Effectue une évaluation de risques initiale, et des évaluations périodiques au besoin, et communique les résultats au conseiller à la sécurité de l'information et aux propriétaires de l'information;
- Assure la sécurité des actifs informationnels, durant tout leur cycle de vie, en déployant les mesures de sécurité appropriées et approuvées par le propriétaire de l'information ;
- Développe, intègre et maintient des mesures de sécurité correspondant au niveau de sensibilité de l'information et autres exigences d'affaires, légales, réglementaires ou contractuelles applicables;
- Appuie le conseiller en sécurité de l'information dans l'élaboration et la mise en œuvre du programme de la sensibilisation à la sécurité de l'information pour les membres du personnel;
- Informe le conseiller à la sécurité de l'information de tout risque important à la sécurité de l'information;
- Élabore et s'assure du respect d'un code d'éthique pour tous les employés spécialisés en technologies de l'information, notamment les développeurs et les administrateurs de réseau.

Utilisateur

- Prend connaissance et adhère aux politiques, règlements, codes de conduite et autres directives pertinentes de HEC Montréal touchant à la sécurité de l'information qui le concernent;
- S'informe et participe activement à la mise en œuvre de la politique;
- Utilise les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont accordés.

3. Définitions

Pour l'application de la présente politique :

Actif informationnel

L'information elle-même, peu importe son support, ainsi que les systèmes utilisés pour son traitement, utilisation, stockage, conservation et communication. La perte, le vol ou la destruction d'un tel actif pourrait causer un préjudice à HEC Montréal. Des exemples d'actifs informationnels sont le dossier *étudiant* et les dossiers des membres du personnel.

Cycle de vie

Période correspondant à la durée de vie de l'information, de sa création ou son acquisition, en passant par son traitement, stockage, transmission, utilisation, jusqu'à sa restitution, destruction ou archivage.

Gestion des risques à la sécurité de l'information

Approche systématique permettant aux gestionnaires de prendre des décisions éclairées en contexte d'incertitude, en considérant les enjeux importants liés aux risques à la sécurité de l'information.

Information

Renseignement consigné sur un support quelconque (papier ou électronique) ou communiqué dans un but de transmission des connaissances. À titre d'exemple, l'information comprend les fichiers structurés (bases de données) et non structurés (fichiers Word, Excel, PowerPoint, PDF, etc.), les courriels, les messages texte, les communications et les messages vocaux, photos, dessins, télécopies, originaux et copies de documents papier, rapports informatisés ainsi que les copies de sauvegarde et les archives.

Intervenant

Tout individu, service ou organisation ayant un rôle défini dans la présente politique ou un tiers ayant des responsabilités spécifiques en matière de sécurité de l'information.

Propriétaire de l'information

Le propriétaire de l'information est la personne désignée par le directeur d'une unité administrative. Il s'assure notamment :

- qu'une classification hiérarchique, selon le degré de risque, est établie et est adéquate pour l'information traitée.
- que le classement de toute l'information stockée est effectué selon les catégories établies et qu'un inventaire de chacune des catégories d'information est tenu.
- que des mesures de protection adéquates sont mises en place pour chaque type d'information.
- qu'une vérification périodique est faite pour s'assurer que l'information continue d'être classifiée adéquatement et que les mesures de protection demeurent valides et efficaces.

Risques à la sécurité de l'information

Tout événement, comportant un degré d'incertitude, qui pourrait porter atteinte à la confidentialité, l'intégrité ou la disponibilité de l'information et causer un préjudice à HEC Montréal.

Risques résiduels

Le risque résiduel est le risque qui subsiste après avoir répondu à un risque donné en prenant différentes mesures. Le risque résiduel est aussi la partie du risque que l'École entend conserver volontairement ou qu'elle doit supporter.

4. Cadre législatif et réglementaire

Les exigences concernant la sécurité de l'information sont présentes dans plusieurs lois, règlements et ententes contractuelles applicables à HEC Montréal. De plus, plusieurs documents normatifs (politiques, énoncés, codes, guides, etc.) imposent également des exigences en matière de sécurité de l'information.

- *Charte des droits et libertés de la personne* (art. 5)
- *Code civil du Québec* (art. 3, 35 à 37)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*
- *Loi et Politique-cadre sur la gouvernance et la gestion des technologies de l'information*
- *Loi concernant le cadre juridique des technologies de l'information* (art. 1 à 46)
- *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information, à l'intention des ministères et organismes publics* (art. 8)
- *Énoncé de politique des trois Conseils: Éthique de la recherche avec des êtres humains* (EPTC2), 2010 (ch. 5)
- *Guide des politiques et des programmes, Fondation canadienne pour l'innovation, 2010* (Ch. 5.1.3)
- *Code de conduite des étudiants, HEC Montréal* (art. 1)
- *Règlement régissant l'activité étudiante à HEC Montréal (B.A.A., Certificat, D.E.S., Maîtrise, MBA, Doctorat)* (art. 18 et 19)
- *Politique relative à la gestion des documents actifs, semi-actifs et inactifs, HEC Montréal* (art. VI, E)