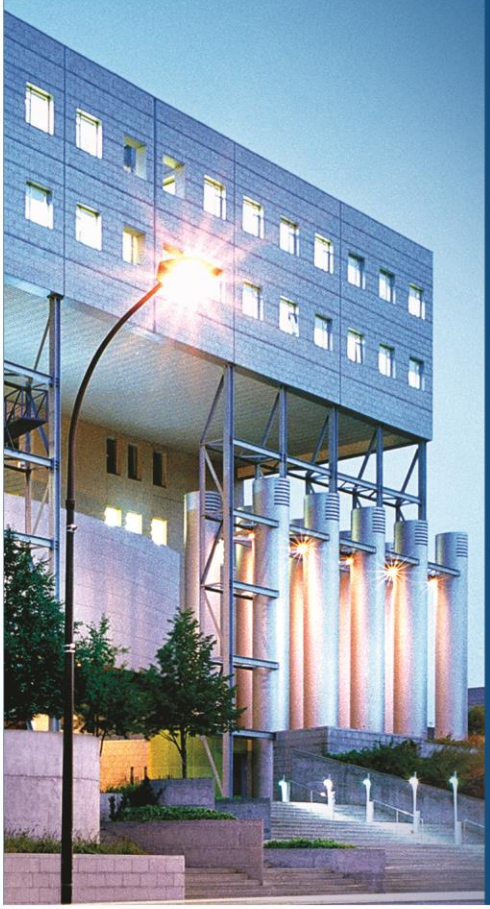
HEC MONTRÉAL

Politique de sécurité de l'information



Adoptée par le Conseil d'administration

le 10 novembre 2011

Mise à jour : 5 décembre 2019

Table des matières

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.

Dans ce contexte, l'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* du Conseil du Trésor du Québec impose des obligations aux établissements universitaires en leur qualité d'organismes publics. Pour répondre à ses obligations réglementaires et législatives, HEC Montréal doit adopter, mettre en œuvre, maintenir à jour et assurer l'application d'une politique de sécurité de l'information qui établit la mise en œuvre de processus formels de sécurité de l'information permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Chapitre I Dispositions générales

Article 1.00 Objectif

1.01 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.

1.02 L'objectif principal de cette politique est d'affirmer 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 de l'information tout au long de son cycle de vie.

Article 2.00 Champ d'application

2.01 La sécurité de l'information est l'affaire de tous. Cette politique s'applique à toute personne physique (enseignant, chercheur, étudiant, diplômé, personnel administratif, retraité, consultant et visiteurs), ou toute personne morale qui utilise ou accède aux ressources informationnelles de HEC Montréal.

2.02 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.

Article 3.00 Principes directeurs

3.01 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) La disponibilité
L'École assure la disponibilité de l'information qu'elle détient de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée. À cette fin, l'École :

(i) S'assure de la fiabilité des processus, des systèmes et des technologies de l'information qui soutiennent les documents;
(ii) Veille à la continuité des services et au maintien des opérations, en dépit de l'occurrence d'événements contraignants ou dommageables;
(iii) Prévoit des solutions de rechange pour assurer la continuité des services jugés essentiels ainsi que le rétablissement des services en cas d'arrêt fortuit;
(iv) S'assure de disposer de mesures d'urgence éprouvées et constamment mises à jour et documentées.

b) L'intégrité
L'École assure l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues. À cette fin, l'École :

(i) Se dote de moyens technologiques ou autres permettant de vérifier que, durant tout leur cycle de vie, l'information des documents essentiels à ses opérations courantes n'a pas été altérée, qu'elle est maintenue dans son intégralité et que le support qui la porte lui procure la stabilité et la pérennité voulue.

c) La confidentialité
L'École s'assure de limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité. À cette fin, l'École :

(i) Ne collige et ne conserve que l'information nécessaire à l'accomplissement de sa mission, dans le respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1) et de la Loi sur les archives (L.R.Q., c. A-21.1);
(ii) Met en place des contrôles et des profils d'accès à l'information, de manière à ce que seuls les personnes, les objets ou les entités technologiques identifiés qui y ont droit et qui sont autorisés puissent y avoir accès, et ce, conformément aux lois et règlements;
(iii) S'assure que les informations, les documents, les équipements, ou le matériel qui sont destinés au rebut, déclarés en bien excédentaire ou confiés à un fournisseur de services pour qu'il procède notamment à leur entretien, à leur recyclage ou à leur destruction, soient traités conformément à la procédure de traitement et de destruction en vigueur. En outre, la destruction des documents dont l'information est devenue désuète ou inutile est effectuée conformément au calendrier de conservation administré par l'École.

d) L'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.

e) 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.

f) La sensibilisation
L'École s'assure d'informer la communauté universitaire des risques et des menaces pouvant affecter l'information afin que ses membres puissent reconnaître les incidents et les risques potentiels et comprendre leurs rôles et responsabilités en matière de sécurité de l'information en développant les habiletés et les compétences appropriées.

Chapitre II Dispositions particulières

Article 4.00 Rôles et responsabilités

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

4.01.01 Conseil d'administration

a) Adopte la politique ainsi que toute modification de celle-ci.

4.01.02 Comité d'audit

a) Supervise le processus de gestion des risques à la sécurité de l'information et l'application de la politique.
b) S'assure de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus.
c) S'assure de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable pour l'organisation.
d) Est informé des actions de l'École en matière de sécurité de l'information, notamment avec le rapport annuel en sécurité de l'information.

4.01.03 Direction de HEC Montréal

a) Valide la politique de sécurité de l'information ainsi que toute modification de celle-ci et recommande au Comité d'audit son adoption par le Conseil d'administration.
b) S'assure de l'application et du respect de la politique par les gestionnaires de l'École.
c) Adopte des mesures visant à favoriser l'application de la politique et des obligations légales de l'École en matière de sécurité de l'information.
d) Détermine les orientations stratégiques, adopte les plans d'action et reçoit les bilans de sécurité de l'information
e) Nomme le responsable de la sécurité de l'information (RSI) tel que requis par la loi.
f) Nomme les coordonnateurs sectoriels de gestion des incidents (CSGI)

4.01.04 Secrétariat général

a) Interprète les lois et règlements pouvant avoir un impact sur la sécurité de l'information.
b) Élabore, diffuse et assure la cohérence des politiques concernant la vie privée, la protection des renseignements personnels et la sécurité de l'information.
c) Valide les clauses contractuelles et s'assure que des mesures adéquates sont prévues afin de protéger l'information et de se conformer à la présente politique en collaboration avec le Service des approvisionnements et le Conseiller en sécurité de l'information.

4.01.05 Comité de sécurité de l'information

a) Agit comme principale instance de concertation en matière de sécurité de l'information de l'École.
b) Formule des recommandations sur le cadre de gestion, les plans d'action et les bilans.
c) Formule toute proposition d'action en matière de sécurité de l'information.

4.01.06 Comité de gouvernance TI

a) Accepte les risques résiduels ayant un niveau d'importance élevé et critique.
b) Fait état à la Direction de HEC Montréal des risques résiduels ayant un niveau d'importance élevé et critique.

4.01.07 Responsable de la sécurité de l'information (RSI)

a) Assiste la direction dans la détermination des orientations stratégiques et des priorités d'intervention.
b) Contribue à la mise en place du cadre normatif des ressources informationnelles et des mesures d'atténuation des risques.
c) Est le premier répondant de l'École au niveau de la sécurité de l'information.
d) Représente le dirigeant d'organisme en matière de déclaration des incidents à portée gouvernementale.
e) Est responsable de la reddition de compte pour satisfaire les exigences législatives et réglementaires
f) Est responsable de l'application de la présente politique.

4.01.08 Conseiller à la sécurité de l'information

a) Élabore la politique de sécurité de l'information et ses mises à jour, et coordonne sa mise en œuvre.
b) Intervient à la mise en œuvre des mesures de réduction des risques.
c) Élabore et met en place des processus officiels de sécurité de l'information.
d) Élabore et met en œuvre le programme de sensibilisation à la sécurité de l'information.
e) Produit un rapport annuel en sécurité de l'information.

4.01.09 Coordonnateur sectoriel de gestion des incidents (CSGI)

a) Contribue à la mise en place du processus de gestion des incidents de sécurité de l'information.
b) Maintien le registre des incidents à la sécurité de l'information.
c) Contribue aux analyses de risques en sécurité de l'information.
d) Gère le processus hiérarchique et de résolution de problème.

4.01.10 Propriétaire d'un système d'information

a) Veille à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de sa direction.
b) Collabore à la catégorisation de l'information sous sa responsabilité et voit à la protection de ces données.

4.01.11 Direction des ressources humaines

a) Vérifie, au besoin, les antécédents des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information;
b) S'assure que les responsabilités des intervenants concernant la sécurité de l'information et le respect de la présente politique, ainsi que du cadre normatif des ressources informationnelles, sont inscrites dans les descriptions de tâches des membres du personnel.
c) Informe et obtient de tout nouvel employé de l'École son engagement au respect de la présente politique.
d) Impose les sanctions appropriées lors de violation des politiques, règlements, directives et code de conduite touchant à la sécurité de l'information.

4.01.12 Direction des technologies de l'information

a) 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 système d'information.
b) Développe, intègre et maintien des mesures de protection correspondant au niveau de sensibilité de l'information et autres exigences d'affaires, légales, réglementaires ou contractuelles applicables lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

4.01.13 Utilisateur

a) Se conforme à la politique de sécurité et à toute directive en matière de sécurité de l'information et d'utilisation des actifs informationnels.
b) Respecte les mesures de sécurité en place, sans les contourner, les désactiver ou les modifier.

Chapitre III Mesures administratives et sanctions

Article 5.00 En cas de contravention à la présente politique

5.01 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 ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

5.02 Tout membre de la communauté universitaire qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires internes applicables.

5.03 De même, toute contravention par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe l'expose aux sanctions prévues au contrat le liant à l'École ou en vertu des dispositions de la législation applicable en la matière.

5.04 Lorsqu'une vérification ou une enquête donne lieu de croire qu'une infraction à une loi ou un règlement a été commise, le directeur des technologies de l'information, en collaboration avec le secrétaire général, peut aussi référer le dossier à toute autre autorité compétente pour vérifier notamment s'il y a matière à poursuite. Il peut alors transmettre à cette autorité les informations colligées au cours de cette vérification ou de cette enquête.

Toute contravention à la présente politique peut entraîner, en plus des mesures prévues aux lois, règlements, politiques ou ententes, les conséquences suivantes, en fonction de la nature, de la gravité et des répercussions du geste ou de l'omission :

a) L'annulation des privilèges d'accès aux actifs informationnels de l'École. L'annulation peut être effectuée sans préavis selon la nature et la gravité de la contravention.
b) L'obligation de remboursement à l'École de toute somme que cette dernière serait dans l'obligation de défrayer à la suite d'une utilisation non autorisée, frauduleuse, ou illicite de ses services ou de ses actifs informationnels.

Chapitre IV Dispositions finales

Article 6.00 Révision

6.01 La politique est révisée au besoin ou selon l'évolution des obligations législatives et réglementaires afin de tenir compte des nouvelles orientations gouvernementales ainsi que l'évolution des pratiques en sécurité de l'information.

Article 7.00 Mise en application et suivi de la politique

7.01 Le responsable de la sécurité de l'information est chargé de l'application de la présente politique.

Article 8.00 Entrée en vigueur

8.01 La présente politique entre en vigueur à la date de son adoption par le Conseil d'administration**.** Elle remplace, à compter de cette date, celle en vigueur depuis le 11 novembre 2011.

Chapitre V 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 sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
- Loi concernant le cadre juridique des technologies de l'information (art. 1 à 46)
- Loi sur les archives
- 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)