POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Document officiel diffusé par le Secrétariat général

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

ADOPTION (INSTANCE/AUTORITÉ)	DATE	RÉSOLUTION
Conseil d'administration	2018-09-27	CAD-1087-5538

AMENDEMENT (S) ET ABROGATION (S)		

CLASSIFICATION	Gestion des ressources informationnelles
COTE	P-INFO-8
ENTRÉE EN VIGUEUR	2018-09-27
RESPONSABLE DE L'APPLICATION	Directrice ou Directeur de l'administration et des ressources

HISTORIQUE

TABLE DES MATIÈRES

1 ÉNONCÉ DE PRINCIPE ET OBJECTIFS

La présente *Politique de sécurité de l'information* vise à montrer l'engagement et la détermination de l'École Polytechnique de Montréal (« Polytechnique ») à protéger l'information qu'elle produit, traite et stocke en vue de la réalisation de sa mission. Polytechnique reconnait qu'elle détient des actifs informationnels qui sont assujettis à un ensemble de lois et de règlements auxquels elle doit se conformer dans le cadre de ses activités.

La présente politique, élaborée conformément aux exigences légales et selon les bonnes pratiques, énonce des principes directeurs qui encadrent la sécurité de l'information au sein de Polytechnique. Elle précise les rôles et responsabilités des intervenantes et intervenants en vue d'une gestion holistique de la sécurité de l'information.

La présente politique vise à assurer :

- La conformité aux lois, règlements et politiques applicables ;
- La disponibilité, l'intégrité et la confidentialité des actifs informationnels ;
- L'identification, la réduction et le contrôle des risques pouvant affecter les actifs informationnels de Polytechnique.

2 CADRE DE RÉFÉRENCE

- *Charte des droits et libertés de la personne* (RLRQ, chapitre C-12, 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 du Québec* (RLRQ, chapitre A-2.1) ;
- *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, chapitre C-1.1) ;
- Commission d'accès à l'information du Québec, *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information, à l'intention des ministères et organismes publics*, en ligne (décembre 2002, mis à jour août 2015, art. 8) ;
- *Politique sur les données institutionnelles de Polytechnique* ;
- *Règlement concernant l'utilisation et la gestion des ressources informatiques* de Polytechnique.

3 CHAMPS D'APPLICATION

Cette politique s'applique

- Aux actifs informationnels de Polytechnique durant tout leur cycle de vie, peu importe leur forme, leur support et leur emplacement. Ces actifs informationnels incluent :
  - Les actifs informationnels appartenant à Polytechnique et détenus par elle ;
  - Les actifs informationnels appartenant à Polytechnique, mais détenus par un partenaire, fournisseur ou autre intervenant ; et
  - Les actifs informationnels utilisés par un consultant, un fournisseur, un partenaire, un organisme ou une firme externe et détenus par lui au bénéfice ou pour et au nom de Polytechnique ; et
- À tous les utilisateurs des actifs informationnels de Polytechnique.

4 DÉFINITIONS

« Actifs informationnels » : Toute information ou donnée, quel que soit son support.

Constitue notamment un actif informationnel un document, une base de données ou une application.

« Catégorisation » : Processus permettant de déterminer le niveau de criticité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs sur Polytechnique, sa clientèle, ses partenaires ou des tiers.

« Fiduciaire de données institutionnelles » : Unité de Polytechnique d'où origine et qui est responsable d'un ensemble de données institutionnelles[1] relatives à sa fonction.

« Incident » : Violation ou menace imminente de violation de la politique, des règlements et directives en sécurité de l'information.

« Unité » : Toutes les unités administratives, d'enseignement et de recherche de Polytechnique, telles qu'elles apparaissent à l'organigramme officiel, incluant les instituts de recherche.

« Utilisateur » : Les utilisateurs sont :

- Les membres des corps étudiant, enseignant et non enseignant de Polytechnique ;
- Les consultants, fournisseurs, partenaires, organismes, firmes externes et toutes les autres personnes qui accèdent à ou utilisent les actifs informationnels de Polytechnique.

5 PRINCIPES DIRECTEURS

Les principes suivants guident la démarche de Polytechnique afin de régir le fonctionnement, l'organisation et la gestion de la sécurité de l'information :

SEC-PD1	S'appuyer sur la famille des normes internationales ISO-27000 qui proposent les meilleures pratiques pour mettre en place une approche de gestion de la sécurité de l'information ;
SEC-PD2	Utiliser une approche de gestion de risque afin d'aligner les mesures de sécurité sur les risques auxquels l'organisation est exposée ;
SEC-PD3	S'assurer de connaître suffisamment les actifs informationnels à protéger ainsi que leur degré de sensibilité et en identifier les responsables ;
SEC-PD4	Effectuer la catégorisation des actifs informationnels de Polytechnique afin d'y aligner les mesures de protection.
SEC-PD5	Attribuer des rôles et des responsabilités claires aux intervenantes et intervenants de l'organisation pour la mise en place d'un cadre de gestion interne de la sécurité permettant une reddition de comptes adéquate ;
SEC-PD6	Protéger, de façon adéquate, les actifs informationnels de Polytechnique des risques et menaces pouvant affecter leur disponibilité, leur intégrité ou leur confidentialité en fonction de leur sensibilité tout au long de leur cycle de vie ;

[1] Voir définition à l'article 6.1 de la *Politique sur les données institutionnelles*.

SEC-PD7	Mettre en place un cadre normatif de gestion de la sécurité de l'information évolutif qui décrive l'ensemble des mesures, normes, processus, procédures ou guides traitant de ce sujet ;
SEC-PD8	Effectuer des vérifications de l'existence et de l'efficacité des mesures de sécurité entourant les actifs informationnels, afin de s'assurer du respect des exigences énoncées dans le cadre normatif de sécurité de l'information ;
SEC-PD9	Sensibiliser et faire participer activement l'ensemble de la communauté de Polytechnique dans la protection des actifs informationnels et favoriser leur utilisation responsable ;
SEC-PD10	Veiller à ce que la gestion de la sécurité de l'information soit faite en conformité avec les exigences légales, réglementaires et contractuelles applicables ainsi qu'avec les règlements et politiques ;

6 STRUCTURE FONCTIONNELLE

6.1 La Directrice ou le Directeur de l'administration et des ressources

La Directrice ou le Directeur de l'administration et des ressources est responsable de :

- Superviser le processus de gestion des risques à la sécurité de l'information et l'application de la politique ;
- Rendre compte, au besoin, aux instances de Polytechnique, dont son Conseil d'administration.

6.2 La ou le responsable de la sécurité de l'information (RSI)

La personne responsable de la sécurité de l'information doit :

- Proposer, coordonner la mise en place et mettre à jour :
  - La présente *Politique de sécurité de l'information* ;
  - Le plan directeur de sécurité de l'information, qui regroupe l'ensemble des initiatives de sécurité de l'information à réaliser ainsi que la feuille de route pour appuyer Polytechnique dans l'atteinte de ses objectifs ;
  - Le cadre normatif de la sécurité de l'information, tel que décrit en annexe 1 ;
  - Le programme de sensibilisation sur la sécurité de l'information, qui présente les activités de sensibilisation ainsi que les moyens à utiliser pour informer la communauté de Polytechnique sur les enjeux de sécurité de l'information.
- Assister les unités dans l'évaluation et la gestion des risques à la sécurité de l'information, tout en leur permettant d'atteindre leurs objectifs d'affaires ;
- Assister les fiduciaires des données institutionnelles dans la catégorisation des actifs informationnels ;
- Analyser toutes demandes de dérogation à un règlement, une politique, une directive, une procédure ou un avis du cadre normatif de sécurité de l'information qui lui seraient soumises ;
- Coordonner les réunions du Comité de sécurité de l'information constitué par la présente Politique ;
- Communiquer au Comité de coordination les risques à la sécurité de l'information et rendre compte de l'application de la présente politique ;

- Diriger, gérer et assurer la mise en place d'encadrements de sécurité de l'information énoncés dans le cadre normatif régissant la sécurité de l'information (règlements, politiques, directives, procédures et avis) ;
- Assurer le suivi de la mise en œuvre de toute recommandation découlant d'une vérification externe ou interne touchant la sécurité de l'information ;
- Effectuer des vérifications de l'existence et de l'efficacité des mesures de sécurité entourant les actifs informationnels, afin de s'assurer du respect des exigences énoncées dans le cadre normatif régissant la sécurité de l'information dans les activités opérationnelles ;
- Coordonner la mise en œuvre des processus de sécurité de l'information aussi bien au niveau des opérations que dans les projets ;
- S'assurer de la conformité du programme de sécurité avec les exigences légales et réglementaires ;
- Contribuer au processus d'acquisition de biens et de services afin de s'assurer que les ententes de services et les contrats intègrent des dispositions permettant de respecter les exigences en matière de sécurité de l'information ;
- Veiller à l'intégration des exigences de sécurité dans les projets impliquant les technologies de l'information ;
- Coordonner la gestion des incidents de sécurité ;
- Effectuer la vigie de sécurité de l'information.

6.3 Le comité de sécurité de l'information

Sous la responsabilité de la Directrice ou du Directeur de l'administration et des ressources, le comité assure le leadership dans la protection des actifs informationnels. Il se réunit une fois par trimestre, et au besoin. Il a pour rôle :

- De proposer les objectifs du programme de sécurité de l'information ;
- De recommander aux instances l'adoption du programme de sécurité de l'information proposé par la ou le responsable de la sécurité de l'information ;
- D'examiner le rendement et l'efficacité du programme de sécurité de l'information et émettre des recommandations ;
- De proposer les ajustements aux encadrements (règlements, politiques, directives, procédures et avis) du cadre normatif de sécurité de l'information ;
- Sur demande soumise par la ou le responsable de la sécurité de l'information, de recommander la mise en place d'une dérogation à la personne responsable de l'application d'une directive, d'une procédure ou d'un avis du cadre normatif de sécurité de l'information ;
- D'examiner, prioriser et recommander aux instances les orientations, initiatives ainsi que les projets de sécurité de l'information.
- D'approuver la catégorisation des actifs informationnels proposée par les fiduciaires des données institutionnelles ;

La composition du Comité est déterminée par la Directrice ou le Directeur de l'administration et des ressources et doit être représentative de la communauté.

6.4 Les fiduciaires de données institutionnelles (FDI)

La dirigeante ou le dirigeant de l'unité fiduciaire des données institutionnelles, ou toute autre personne qu'il désigne (ci-après la ou le « **fiduciaire des données institutionnelles** »), exerce les rôles et responsabilités décrites dans la *Politique sur les données institutionnelles*.

De plus, la ou le fiduciaire des données institutionnelles doit s'assurer :

- Qu'une catégorisation hiérarchique, selon le degré de risque, est établie et est adéquate pour l'information traitée ;
- Que la catégorisation de toute l'information stockée est effectuée selon les catégories établies et la tenue d'un inventaire de chacune des catégories d'information ;
- De proposer une catégorisation des actifs informationnels sous sa responsabilité au comité de sécurité de l'information ;
- Que des mesures de protection adéquates sont mises en place pour chaque type d'information ; et
- Qu'une vérification périodique est faite pour s'assurer que l'information continue d'être catégorisée adéquatement et que les mesures de protection demeurent valides et efficaces.

6.5 Les unités

Les unités doivent :

- Participer à l'évaluation des risques à la sécurité de l'information ;
- Conserver la responsabilité de la protection des actifs informationnels, même lorsque cette dernière est déléguée à un tiers ;
- Gérer les contrats et la relation avec les fournisseurs pour tout aspect touchant à la sécurité de l'information, en collaboration avec la ou le Responsable de la sécurité de l'information ;
- S'assurer que les actifs informationnels respectent la catégorisation établie par les FDI ;
- Informer et sensibiliser toute personne sous leur responsabilité de l'importance de la sécurité de l'information et de l'existence de la présente politique et des autres directives applicables ;
- Communiquer tout risque important à la sécurité de l'information à la ou au Responsable de la sécurité de l'information.

6.6 Le Secrétariat général

Le Secrétariat général :

- Interprète les lois et règlements pouvant avoir un impact sur la sécurité de l'information ;
- Communique les exigences légales, réglementaires et contractuelles applicables au Responsable de la sécurité de l'information, aux fiduciaires des données institutionnelles et aux autres intervenants, au besoin ;
- Valide les clauses contractuelles touchant à la sécurité de l'information, en collaboration avec la ou le Responsable de la sécurité de l'information ;
- Révise tous nouveaux documents officiels, au sens de la *Directive sur les documents officiels*, touchant à la sécurité de l'information ainsi que toute modification à ces documents.

6.7 La Direction des ressources humaines

La Direction des ressources humaines :

- Informe et obtient de tout employé de Polytechnique son engagement au respect de la présente Politique et du cadre normatif en découlant ;
- Participe à la mise en place des programmes de sensibilisation et d'information des employés de Polytechnique en matière de sécurité de l'information.

6.8 Les utilisateurs

La responsabilité de la protection des actifs informationnels incombe à tous les utilisateurs. Chacun d'eux est responsable de respecter la politique ainsi que tous les autres documents du cadre normatif de sécurité de l'information.

À cette fin, les utilisateurs doivent notamment :

- Prendre connaissance et adhérer à la présente Politique ;
- Utiliser les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui leur sont autorisés.

7 DISPOSITIONS FINALES

7.1 Mise en œuvre et suivi

La ou le Responsable de la sécurité de l'information est responsable de la coordination, de la mise en œuvre et de la mise à jour de la présente politique.

7.2 Modifications mineures

La Directrice ou le Directeur de l'administration et des ressources peut apporter des modifications mineures à la présente politique. Les membres du Conseil d'administration sont informés de cette modification à une réunion ultérieure**.**

Toute modification aux annexes, le cas échéant, est considérée comme une modification mineure.

7.3 Langage inclusif

La présente directive est rédigée en langage inclusif de manière à désigner les personnes de tout genre et de toute identité de genre.

7.4 Entrée en vigueur

La présente politique entre en vigueur le27 septembre 2018.

ANNEXE 1 CADRE NORMATIF DE LA SÉCURITÉ DE L'INFORMATION

Le cadre normatif de la sécurité de l'information de Polytechnique est composé des règlements, politiques, directives et avis qui traitent des questions reliées à la sécurité des actifs informationnels de Polytechnique. Ce cadre traitera sans s'y limiter des sujets suivants :

- Politique de sécurité de l'information
- Surveillance et journalisation des systèmes d'information
- Gestion des accès
- Gestion des incidents de sécurité
- Architecture de sécurité d'entreprise
- Protection des renseignements personnels
- Développement sécuritaire des systèmes
- Catégorisation des actifs informationnels
- Chiffrement des données
- Sécurité dans les relations avec les tiers
- Sécurité physique
- Sécurité dans la continuité des affaires