BCI
BUREAU DE
COOPÉRATION
INTERUNIVERSITAIRE

Politique sur la sécurité de l'information

Adoptée par le Conseil d'administration, le 9 octobre 2020

Entrée en vigueur : 9 octobre 2020

Révisée le : _____

500, rue Sherbrooke Ouest
Bureau 200
Montréal QC H3A 3C6

T 514 288.8524
info@bci-qc.ca
bci-qc.ca

Table des matières

1. Préambule

Le Bureau de coopération interuniversitaire (le « **BCI** ») reconnaît l'apport grandissant des technologies de l'information à ses activités, notamment en ce qui a trait aux communications, ainsi que l'importance et la valeur de ses documents et de l'information que ceux-ci comportent en regard de la continuité de ses opérations.

Le BCI détient par ailleurs des informations confidentielles, notamment des renseignements personnels, dont la gestion et l'utilisation font l'objet d'un encadrement légal.

2. Définitions

Dans la présente politique, à moins que le contexte n'impose un sens différent, les expressions et mots suivants signifient :

Actif informationnel : tout Document ou Système;

Document : toute information portée par un support quel qu'il soit;

Incident de sécurité : tout événement ou occurrence, incluant un manquement à cette Politique, à une directive ou mesure de sécurité qui entraîne une atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'un Actif informationnel;

Intervenant : toute instance, personne ou groupe de personnes ayant un rôle et des responsabilités spécifiques en matière de sécurité de l'information;

Utilisateur : tout intervenant, administrateur, dirigeant, employé, mandataire ou fournisseur du BCI et leur représentant, le cas échéant, les membres de comités, sous-comités et groupes de travail, les partenaires externes, les invités, les organismes ou firmes externes autorisées à accéder, à utiliser, ou à traiter l'Actif informationnel du BCI;

Système : tout réseau, ordinateur, équipement, logiciels, unité de stockage, base de données ou autre faisant ou non appel aux technologies de l'information, destiné à créer, communiquer, traiter, conserver ou détruire un document.

3. Objectif

La présente Politique sur la sécurité de l'information (la « **Politique** ») énonce des mesures de protection administratives, techniques et physiques conçues pour :

- Assurer la conformité légale et réglementaire des pratiques et processus du BCI en regard de la sécurité de l'information;
- Établir les orientations et principes généraux destinés à assurer efficacement la sécurité de l'information, ainsi que la continuité des opérations, et de façon plus spécifique :
  - Assurer le maintien de l'intégrité de l'information;
  - Assurer le maintien de la confidentialité des informations qui revêtent un tel caractère;
  - Assurer le maintien de l'accessibilité de l'information;

- Assurer la cohérence des directives et mesures relatives aux Actifs informationnels et à la gestion des risques relatifs à la sécurité de l'information;
- Sensibiliser les Utilisateurs à l'importance de la sécurité de l'information et aux risques relatifs à celle-ci, en énonçant les rôles et responsabilités de chacun à cet égard.

4. Application et portée

La Politique s'applique à tous les Utilisateurs.

Cette Politique s'applique à tous les Actifs informationnels générés, conservés, reçus, communiqués ou utilisés par le BCI que ceux-ci soient la propriété du BCI ou l'objet d'une entente de services ou d'impartition avec un fournisseur tiers. Dans ce dernier cas, les ententes contractuelles devront imposer des obligations aux fournisseurs de services permettant de satisfaire aux exigences de la présente Politique.

5. Principes directeurs

5.1 Approche globale

Les procédures, processus, mesures et engagements contractuels du BCI relatifs aux Actifs informationnels doivent être élaborés, implantés et appliqués de façon à en maintenir l'intégrité, assurer leur accessibilité, et à en préserver la confidentialité, de façon à respecter les obligations légales et réglementaires du BCI.

5.2 Inventaire

Le BCI s'assure d'inventorier et classifier ses Actifs informationnels.

5.3 Responsabilité

Chacun des Utilisateurs ayant accès aux Actifs informationnels assume des responsabilités en regard du maintien de la sécurité, et du respect des mesures de sécurité, notamment en regard de la préservation de la confidentialité de ses identifiants, de ses accès aux Actifs informationnels par l'entremise de réseaux externes, et de la sécurité des équipements et support mobiles du BCI, et est redevable de ses actions auprès de la Direction générale.

5.4 Utilisation à des fins professionnelles

Les Actifs informationnels du BCI sont mis à la disposition des Utilisateurs à des fins d'usages professionnels dans le cadre de l'exercice de leurs fonctions.

5.5 Droits d'accès

Les droits d'accès aux Actifs informationnels sont accordés de façon restreinte aux Utilisateurs en fonction de leurs responsabilités et de leurs tâches.

5.6 Protection des renseignements personnels

L'accès et l'utilisation des renseignements personnels recueillis par le BCI doivent être contrôlés et ne doivent être autorisés qu'aux fins pour lesquelles ils ont été recueillis ou obtenus, le tout conformément à la Politique sur la protection des renseignements personnels et aux dispositions législatives applicables.

5.7 Engagements contractuels

Toute entente contractuelle conclue avec un fournisseur de services relativement aux Actifs informationnels ou susceptible d'entraîner un impact sur les Actifs informationnels doit contenir des stipulations imposant aux fournisseurs des obligations permettant de rencontrer les exigences de la présente Politique et qui soient conformes aux mesures de sécurité appliquées par le BCI.

5.8 Mesures de sécurité

Le BCI a mis et mettra en place des mesures de protection, de prévention, de détection, d'assurance et de correction dans le but d'assurer la confidentialité, l'intégrité, et l'accessibilité des Actifs informationnels, ainsi que le contrôle d'accès, l'authentification des Utilisateurs, de même que la continuité des opérations. Les mesures doivent également viser à empêcher les Incidents de sécurité, les erreurs, la malveillance, ainsi que les atteintes à la confidentialité, à l'intégrité ou à la disponibilité des Actifs informationnels.

5.9 Surveillance

Le BCI peut contrôler, surveiller, vérifier et enregistrer tout accès, communication, ou utilisation des Actifs informationnels faits par les Utilisateurs du BCI afin de s'assurer d'une utilisation adéquate des Actifs informationnels et du respect de la présente Politique et des mesures de sécurité.

5.10 Sensibilisation et formation

Le BCI doit mettre en œuvre et appliquer un programme de sensibilisation et de formation à la sécurité des Actifs informationnels.

5.11 Évolution

Une évaluation périodique des risques et des mesures de sécurité des Actifs informationnels doit être effectuée afin de s'assurer de leur adéquation.

6. Rôles et responsabilités

6.1 Rôles et responsabilités des Intervenants du BCI

6.1.1 Conseil d'administration

- Adopte cette Politique et de toute modification à celle-ci;
- S'assure de la bonne gouvernance de la sécurité de l'information, incluant la gestion adéquate des risques à la sécurité de l'information.

6.1.2 Comité exécutif

- Adopte les directives et mesures relatives à la sécurité de l'information ainsi que toute modification à celles-ci.

6.1.3 Direction générale

- Supervise l'élaboration de toute directive ou mesure ainsi que toute modification à celles-ci ou à cette Politique et recommande leur adoption, selon le cas, au Conseil d'administration ou au Comité exécutif;
- S'assure de l'application de la Politique et des directives, et affecte les ressources nécessaires à cette fin;
- Nomme les membres du Comité de sécurité de l'information;
- Supervise les travaux du Comité de sécurité de l'information;
- Communique aux Utilisateurs du BCI le contenu de cette Politique et des directives qui en découlent;
- Supervise les initiatives de sensibilisation des Utilisateurs à la sécurité de l'information.

6.1.4 Comité de sécurité de l'information

Sous la supervision de la Direction générale, le Comité de sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information au sein du BCI. Ses principales responsabilités sont de :

- Élaborer toute directive et mesure ainsi que toute modification à celles-ci ou à cette Politique et formuler des recommandations à la Direction générale;
- Coordonner la mise en œuvre de cette Politique et de toute directive et mesure;
- Élaborer et recommander à la Direction générale des initiatives de sensibilisation à la sécurité de l'information ainsi que toute communication à transmettre aux Utilisateurs et relativement à cette Politique et à ses directives;
- Développer les processus de gestion des risques relatifs à la sécurité de l'information. Entre autres, il identifie les événements susceptibles de constituer des Incidents de sécurité.

Sont membres du Comité sur la sécurité de l'information :

- Un représentant de la Direction des technologies de l'information;
- Un administrateur réseau de la Direction des technologies de l'information et en charge de la sécurité informatique;
- Un responsable de la gestion des ressources humaines;
- Un ou des représentants des employés du BCI désignés par la Direction générale selon leurs fonctions au sein du BCI;
- Un responsable des affaires juridiques;
- Le responsable de la protection des renseignements personnels;
- Un responsable de la gestion documentaire;
- Un responsable de la gestion des incidents.

De plus, la Direction générale peut inviter toute personne à participer au comité en fonction des besoins établis ou d'expertises spécifiques.

6.1.5 Direction des technologies de l'information (TI)

- Assure la sécurité des Actifs informationnels sur support technologique, durant leur cycle de vie, en déployant les mesures de sécurité appropriées et approuvées par la Direction générale;
- Met en œuvre les directives et mesures relatives à la sécurité des Actifs informationnels sur support technologique;
- Surveille l'application des directives et mesures de sécurité et avise la Direction générale de tout manquement ou événement susceptible de constituer ou d'entraîner un Incident de sécurité et formule toute recommandation visant à assurer une saine gestion des risques à la sécurité des Actifs informationnels sur supports technologiques;
- Assure la mise en œuvre de toutes mesures correctives appropriées à la suite d'un Incident de sécurité de l'information sur approbation de la Direction générale;
- Maintient le registre des Incidents à la sécurité de l'information.

6.1.6 Responsable des ressources humaines

- Met en œuvre les directives et mesures relatives à la sécurité de l'information qui concernent les processus d'embauche et l'application des mesures de sécurité physique;
- Intervient auprès des employés concernés en cas de manquement à cette Politique ou aux directives ou mesures de sécurité de l'information, en collaboration avec la Direction des TI et le supérieur immédiat de cet employé;
- 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 profils d'accès aux Actifs informationnels.

6.1.7 Responsable de la gestion documentaire

- Met en œuvre les mesures de sécurité relative à la gestion des Documents semi-actifs des archives du BCI;
- Assure la destruction sécuritaire des Documents du BCI, lorsque requis par la finalité de l'information ou à la demande des secteurs d'activités.

6.1.8 Responsable des affaires juridiques

- Effectue une veille juridique afin d'assurer la conformité de cette Politique à l'encadrement légal applicable;
- Communique les exigences légales, réglementaires et contractuelles applicables au Comité sur la sécurité de l'information;
- Assure la conformité des ententes contractuelles du BCI relativement à la sécurité de l'information.

6.2 Responsabilités des Utilisateurs

La responsabilité de la sécurité de l'information est partagée et incombe à tous les Utilisateurs. Les Actifs informationnels du BCI sont mis à la disposition de l'Utilisateur qui s'engage à les utiliser en conformité avec la présente Politique et les directives. Chaque Utilisateur a la responsabilité d'assurer la sécurité des Actifs informationnels qu'il utilise ou dont il a la possession et d'aviser la Direction générale de tout Incident de sécurité et de tout risque lié à la sécurité de l'information.

6.3 Sanctions

Toute infraction à cette Politique ainsi qu'aux directives est susceptible de sanctions.

Le défaut d'un employé de se conformer à la Politique ainsi qu'à ses directives pourra entraîner des sanctions disciplinaires.

Le défaut d'un administrateur ou dirigeant de se conformer à la Politique est susceptible de constituer un manquement aux règles de gouvernance ou un manquement aux obligations légales ou contractuelles de ceux-ci.

Un manquement attribuable à un fournisseur ou un partenaire externe est susceptible de constituer un défaut contractuel.

Une violation de la Politique ainsi qu'aux directives peut aussi être constitutive d'une infraction légale ou être la cause d'un préjudice économique. Le cas échéant, les recours appropriés pourraient être entrepris ou les autorités compétentes notifiées.

7. Mise en œuvre

La mise en œuvre de cette Politique repose sur une approche globale tenant compte des aspects humains, organisationnels, juridiques et techniques, et commande l'implantation et la coordination de directives et mesures adéquates en regard de la sensibilité des Actifs informationnels.

8. Cadre juridique

Les activités du BCI en regard des Actifs informationnels sont notamment encadrées par :

- les dispositions législatives suivantes :
  - *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P-39.1;
  - *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c. C-1.1;
  - *Code civil du Québec*.
- les politiques et directives suivantes, telles qu'elles seront adoptées :
  - *Politique sur la protection des renseignements personnels*;
  - *Politique sur la gestion documentaire*;
  - *Directive sur l'utilisation des actifs informationnels*;
  - *Directive relative au plan d'intervention et de gestion d'un incident de sécurité de l'information*;
  - *Directive relative aux contrôles et mesures de sécurité de l'information*.

9. Entrée en vigueur et révision

Cette Politique entre en vigueur dès son adoption par le Conseil d'administration du BCI. Elle sera révisée tous les trois ans, ou plus tôt en cas de modification au cadre juridique ou d'évolution technologique ayant une incidence sur son application.

Toute modification à cette Politique doit être adoptée par le Conseil d'administration.