SÉCURITÉ DE L'INFORMATION

Adoption
Date : CE 18/02/2020
BG 25/02/2020

Modifications
Date : CG 17/11/2022
BG 29/11/2022

Ce document remplace tout règlement antérieur en cette matière.

Prochaine révision : 2027

SOMMAIRE

1. Énoncé de la politique

1.1 La présente politique encadre le programme de sécurité de l'information (« programme ») de l'Université de Saint-Boniface (« Université ») ainsi que les procédures administratives connexes, lesquelles ont pour but de protéger les actifs informationnels sensibles de l'Université — quels qu'en soient la forme ou le propriétaire — contre l'accès, l'utilisation, la divulgation, l'interruption, la modification, l'inspection, l'enregistrement ou la destruction non autorisés. Le programme vise ainsi à protéger l'Université et les personnes qui lui confient des renseignements personnels ou une propriété intellectuelle contre toute conséquence néfaste découlant du traitement inapproprié de ces données.

1.2 L'Université s'engage à créer et à maintenir un milieu où les membres de sa communauté peuvent avoir la certitude que la cueillette, la consultation, le traitement, le stockage et le transfert de leurs renseignements personnels, des renseignements institutionnels et de la propriété intellectuelle s'effectuent de façon sécurisée et appropriée.

1.3 L'Université s'engage à satisfaire aux exigences juridiques et règlementaires provinciales et fédérales qui s'appliquent aux entités semblables dans le milieu postsecondaire.

2. Champ d'application

2.1 Tous les membres de la communauté universitaire doivent adhérer à la présente politique.

3. Modalités de la poltique

3.1 La politique du programme, de même que les procédures et processus connexes, s'appliquent à l'ensemble des éléments suivants :

a) des actifs informationnels sensibles — quels qu'en soient la forme, ou le ou la propriétaire — qui sont conservés, utilisés ou transmis par l'Université;

b) des mesures de sécurité que déploie cette dernière pour protéger ces actifs; et

c) des personnes qui les utilisent, sans égard à la méthode ou à l'appareil employés pour y accéder.

3.2 L'Université reconnait que la sécurité de l'information est un processus géré centralement qui, pour être efficace, nécessite l'engagement de tous les membres de l'équipe de direction (propriétaires de l'information), des mesures de sécurité appropriées compte tenu du niveau de classification de l'information protégée et des efforts de sensibilisation continus en matière de sécurité.

3.3 L'Université veuille à ce que la senbilisation en matière de sécurité de l'information soit intégrée à la culture institutionnelle en ayant recours à l'éducation, à la formation et à la mise en place des mesures techniques et physiques visant à prévenir une utilisation inappropriée et accidentelle du réseau de l'Université ou de ses actifs informationnels.

4. Définitions

4.1 **Actif informationnel** : inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles contenant des renseignements sensibles ou confidentiels de l'Université.

4.2 **Le Comité sur la sécurité de l'information :** se compose des membres de l'équipe de direction (« propriétaires d'information ») qui ont la responsabilité des données sensibles au sein de leur unité ou des approbations connexes.

4.3 **Propriétaire de l'information :** personne désignée par le vice-recteur ou la vice-rectrice à l'administration et aux finances qui détermine l'accès aux actifs informationnels de l'unité dont elle a la responsabilité.

4.4 **Responsable de l'information :** personne qui est chargée de la gestion et de la coordination de tous les aspects de la sécurité de l'information avec l'appui du Service des technologies de l'information et du Service des installations et de la sécurité.

5. Responsabilités

5.1 Le Bureau des gouverneurs est chargé de l'approbation de la politique sur la sécurité de l'information.

5.2 La rectrice ou le recteur est chargé de l'approbation des procédures qui composent le programme.

5.3 La vice-rectrice ou le vice-recteur à l'administration et aux finances est responsable de :

5.3.1 communiquer, administrer, interpréter et réviser la présente politique;

5.3.2 présider le Comité sur la sécurité de l'information;

5.3.3 recevoir le rapport annuel détaillé des résultats des audits et des contrôles en place et faire un rapport sommaire des résultats au Comité sur la sécurité de l'information.

5.4 Le Comité sur la sécurité de l'information se réunit au moins une fois par année et est responsable de :

5.4.1 recommander à la rectrice ou au recteur les exceptions aux procédures du programme dont la nécessité est démontrée et documentée, et, le cas échéant, de gérer les exceptions autorisées;

5.4.2 revoir le rapport annuel des résults des audits et des contrôles en place et faire des recommandations appropriées;

5.4.3 revoir les procédures de la sécurité de l'information.

5.5 Le ou la responsable de l'information coordonne les activités du comité et lui sert de personne-ressource principale. Il ou elle est responsable de :

5.5.1 fournir son expertise et offrir les formations en matière de sécurité de l'information;

5.5.2 auditer et valider les contrôles en place;

5.5.3 faire un rapport annuellement des résultats des audits et des contrôles en place au Comité sur la sécurité de l'information;

5.5.4 coordonner les activités du Comité sur la sécurité de l'information.

5.6 Les propriétaires d'information sont chargés de trancher les questions concernant la classification des données à l'égard de chaque actif informationnel sous leur responsabilité respective; à cette fin, ces personnes sont les principaux responsables de la classification des renseignements dont la propriété leur a été assignée. Chaque propriétaire d'information est responsable :

5.6.1 d'utiliser le processus et le schéma de classification des données adoptés par l'Université lors de la planification de tout nouveau système d'information ou de toute modification importante d'un tel système, pour identifier toute information présentant des exigences de sécurité accrues;

5.6.2 de conseiller le Comité sur la sécurité de l'information sur les exigences opérationnelles spécifiques aux actifs informationnels sensibles repertoriés pour faire en sorte que des procédures d'accès appropriées soient en place pour protéger ces renseignements;

5.6.3 d'approuver et d'attribuer les privilèges d'accès à l'égard de chaque usager ou usagère, ou groupe d'usagers qui demande l'accès aux actifs informationnels sensibles qui lui sont assignés;

5.6.4 de s'assurer que chaque usager ou usagère qui a accès à de l'information sensible reçoit la formation sur la sécurité de l'information;

5.6.5 de veiller à ce que des contrôles d'accès physique soient en place et soient respectés dans les zones à sa charge;

5.6.6 de revoir annuellement l'accès des usagers et usagères afin de veiller à ce que les données soient exactes et à jour;

5.6.7 de veiller à ce que les échanges d'information ou les accords de transfert d'information (par moyen électronique ou physique) soient documentés et d'exiger que des mesures de sécurité appropriées soient en place et s'assurer que l'échange ou le transfert soit approuvé, lorsqu'il est question d'actifs informationnels sensibles;

5.6.8 de participer aux examens et aux audits en matière de sécurité.

5.7 Les usagers et usagères sont ceux et celles que les propriétaires d'information ont autorisés à accéder à des renseignements sensibles au sein de leur unité lorsque leur emploi l'exige. Chaque usager ou usagère a les responsabilités suivantes :

5.7.1 suivre la formation de sensibilisation à la sécurité qui est appropriée compte tenu de son rôle, en conformité avec la présente politique et tel qu'exigé par sa superviseure ou son superviseur;

5.7.2 établir le niveau de sensibilité de l'information obtenue et veiller à ce qu'elle soit recueillie d'une façon appropriée à sa classification;

5.7.3 étiqueter les actifs informationnels sous forme papier ou électronique nouvellement acquis qui sont conservés dans les espaces physiques ou numériques de l'Université en utilisant la classification appropriée, dès qu'il est raisonnablement possible de le faire et en utilisant les normes de l'Université;

5.7.4 veiller à ce que tout document physique (y compris les notes manuscrites) servant à documenter un renseignement sensible soit déchiqueté ou conservé à l'Université dans un endroit suffisamment sécurisé (en conformité avec les exigences que prévoient, notamment, la *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur les renseignements médicaux personnels* ainsi que la norme de sécurité des données de l'industrie des cartes de paiement (« norme PCI DSS »));

5.7.5 veiller à ce que tout document, fichier ou dossier virtuel servant à stocker des renseignements sensibles soit conservé sur un appareil ou à un endroit du réseau qui soit suffisamment sécurisé;

5.7.6 veiller à ce que les actifs informationnels nouvellement acquis soient répertoriés dans l'inventaire des actifs informationnels dressé par l'Université, directement ou au moyen d'un processus approuvé de notification;

5.7.7 veiller à ce que les actifs informationnels internes ou confidentiels ne soient pas divulgués à de tierces parties de façon inappropriée;

5.7.8 assurer la protection des clés d'accès comme les cartes d'identité, les jetons électroniques et les mots de passe liés aux comptes qui donnent accès aux renseignements sensibles de l'Université ou aux endroits où ceux-ci sont stockés.

6. Principes directeurs

6.1 Exigences en matière de formation sur la sécurité de l'information

Afin qu'ils soient suffisamment informés sur la sécurité de l'information pour les fins du programme et afin que les formations nécessaires concernant les procédures du programme soient offertes, le personnel de l'Université et les tierces parties qui ont accès à des actifs informationnels sensibles, quels qu'en soient la forme ou le propriétaire et sans égard à la méthode ou à l'appareil employés pour y accéder, doivent :

a) recevoir une formation de sensibilisation sur la sécurité de l'information et une formation sur la politique, les normes et les procédures applicables à la gestion des actifs informationnels sensibles de l'Université, et ce, dès le début de leur emploi et au moyen d'une méthode qui permet de confirmer la participation à la formation;

b) avoir accès aux versions en vigueur de la politique, des normes et des procédures applicables;

c) être informés par l'Université de toute modification apportée à la politique, aux normes et aux procédures relatives à la gestion des actifs informationnels sensibles de l'Université.

6.2 Exceptions à la politique

6.2.1 Déclaration obligatoire en cas de non-conformité

Les actifs informationnels sensibles, quels qu'en soient la forme ou le propriétaire, doivent en tout temps être gérés en conformité avec la politique, les normes et les exigences de l'Université, sans égard à la méthode ou à l'appareil employé pour les conserver ou y accéder. L'accès, l'utilisation, la divulgation, l'interruption, la modification, l'inspection, l'enregistrement ou la destruction non conformes doivent être signalés au ou à la responsable de l'information. Il ou elle signalera l'incident au Comité sur la sécurité de l'information, qui le traitera dès que raisonnablement possible.

Le Comité sur la sécurité de l'information examinera chaque incident et décidera s'il faut remédier à la non-conformité ou, pourvu qu'il y ait un besoin démontré et documenté, recommander une exception pendant une certaine période et revoir la situation à l'expiration de ce délai.

Les exceptions autorisées sont répertoriées à titre de dérogations reconnues dans l'inventaire des actifs informationnels.

6.2.2 Traitement des cas non autorisés de non-conformité

Au moment de leur découverte, les cas non autorisés de non-conformité seront traités en tant qu'atteinte à la sécurité interne. Le ou la responsable de l'information doit veiller à ce que des mesures correctives soient prises, lesquelles peuvent notamment comprendre les mesures suivantes :

a) restreindre l'accès aux services informatiques ou de réseau ou aux ressources liées aux comptes ou aux appareils informatiques (avec l'autorisation de la vice-rectrice ou du vice-recteur à l'administration et aux finances);

b) restreindre l'accès physique aux zones sécurisées (avec l'autorisation de la vice-rectrice ou du vice-recteur à l'administration et aux finances);

c) signaler les incidents aux ressources humaines.

7. Procédures

7.1 Séparation des fonctions

Lorsque des fonctions sont confiées à certains individus, les attributions et les responsabilités qui présentent un conflit doivent être attribuées à d'autres personnes dans le but de réduire les situations où des systèmes d'information pourraient être modifiés ou utilisés de façon non intentionnelle ou non autorisée.

Au minimum, en matière de gestion de la sécurité de l'information à l'Université, les fonctions qui suivent présentent des conflits évidents et doivent être assignées à des rôles ou individus différents :

a) les personnes chargées de prendre une mesure ne peuvent être chargées de l'autoriser;

b) les personnes autorisées à mener des opérations sensibles ne peuvent les auditer;

c) une même personne ne peut être chargée d'un procédé critique en matière de sécurité de l'information du début à la fin;

d) la personne qui utilise un compte ne peut être celle qui l'a créé;

e) la création de comptes possédant des privilèges d'accès élevés à un individu est documentée et approuvée par le ou la propriétaire de l'information qui n'a pas elle-même ou lui-même la capacité de créer de tels comptes;

f) la création de comptes possédant des privilèges administratifs conférant un accès complet à des comptes de plus d'un propriétaire d'information est documentée et approuvée par la ou le responsable de l'information, qui n'a pas elle-même la capacité de créer de tels comptes.

8. Renvois

8.1 *Loi sur l'accès à l'information et la protection de la vie privée*, C.P.L.M. c. F1758.2; *Loi sur les renseignements médicaux personnels*, C.P.L.M. c. P33.5
8.2 La norme de sécurité des données de l'industrie des cartes de paiement (« Norme PCI DSS »)
8.3 Procédure sur la classification de l'information
8.4 Procédure sur le système de classification de l'information
8.5 Procédure sur l'étiquetage et le traitement de l'information selon sa classification
8.6 Procédure sur le contrôle de l'accès fondé sur la classification de l'information