POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

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

Modifications
Date :

SOMMAIRE

1. Objet

Le programme de sécurité de l'information (« programme ») de l'Université de Saint-Boniface (« Université ») est régi par la présente politique sur la sécurité de l'information ainsi que les politiques et 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.

2. Portée

Les politiques du programme, de même que les procédures et processus connexes, s'appliquent à l'ensemble

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. Énoncé de valeurs

3.1 L'Université s'engage à créer et à entretenir 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.

3.2 L'Université s'engage à satisfaire aux exigences juridiques ou règlementaires qui s'appliquent aux entités semblables.

3.3 L'Université reconnait que la sécurité de l'information est un processus géré centralement qui, pour être efficace, nécessite les ressources suivantes : un soutien de la gestion, 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.

3.4 L'Université s'efforce de veiller à ce que les efforts de sensibilisation en matière de sécurité de l'information soient intégrés à la culture de l'Université en ayant recours à l'éducation, à la formation et à la prise des mesures logiques et physiques visant à prévenir une utilisation inappropriée et accidentelle du réseau de l'Université ou de ses actifs informationnels.

4. Énoncés de politique

4.1 Accessibilité des politiques relatives à la sécurité de l'information

Les politiques, normes et procédures liées au programme doivent être conservées dans un endroit central accessible à l'ensemble du personnel ayant accès à des renseignements sensibles de l'Université.

4.2 Rôles et responsabilités en matière de sécurité de l'information

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

La *rectrice* ou le *recteur* est chargé de revoir les politiques qui composent le programme et d'approuver celles qui ne relèvent pas du Bureau des gouverneurs.

Le *Comité sur la sécurité de l'information* se compose des directrices et directeurs, et des doyens et doyennes dont relèvent les données sensibles au sein de leur unité ou les approbations connexes (« propriétaires d'information »). Le Comité est présidé par la *vice-rectrice ou le vice-recteur à l'administration et aux finances* et se réunit au moins une fois par année. Il possède les attributions suivantes :

a) désigner des propriétaires d'information supplémentaires à l'égard de certains actifs informationnels sensibles;

b) recommander à la rectrice ou au recteur, ou au Bureau des gouverneurs, selon le cas, les exceptions aux politiques du programme dont la nécessité est démontrée et documentée, et gérer les exceptions autorisées;

c) revoir les politiques du programme annuellement.

Le ou la *responsable de la sécurité de l'information* coordonne les activités du Comité et lui sert de personne-ressource principale. Il ou elle possède les attributions suivantes :

a) offrir son expertise en matière de sécurité de l'information;

b) auditer et valider les contrôles en place;

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

Les *propriétaires d'information* sont chargés de trancher les questions concernant la classification des données à l'égard de chaque actif informationnel; 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 possède les attributions suivantes :

a) utiliser la procédure et le schéma afférents à la classification des données, désigner les renseignements visés par des exigences de sécurité supérieures au cours de la planification de tout nouveau système d'information ou de toute modification importante d'un tel système;

b) orienter le Comité sur la sécurité de l'information relativement aux exigences opérationnelles spécifiques aux actifs informationnels sensibles repertoriés pour faire en sorte que des politiques d'accès appropriées soient en place pour protéger ces renseignements;

c) approuver et 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;

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

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

f) veiller à ce que les accords d'échange ou de transfert d'information (par moyen électronique ou physique) soient documentés, exigent que des mesures de sécurité appropriées soient en place (en conformité avec la politique interne) et soient approuvés, lorsqu'il est question d'actifs informationnels sensibles;

g) participer aux examens et aux audits en matière de sécurité.

Les *usagers* et *usagères* sont ceux 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 :

a) suivre la formation de sensibilisation à la sécurité qui est appropriée compte tenu de son rôle, en conformité avec la présente politique sur la sécurité de l'information, et que demande le personnel supérieur;

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

c) étiqueter les actifs informationnels nouvellement acquis qui sont conservés dans les locaux et le matériel appartenant à l'Université (y compris les ressources en matière d'informatique et de réseau) au moyen de la classification appropriée, dès qu'il est raisonnablement possible de le faire et en utilisant les normes de l'Université applicables aux noms des dossiers (au moment de la sauvegarde du document et au moyen d'étiquettes physiques avant le stockage physique du document);

d) 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]);

e) 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;

f) 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;

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

h) 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.

4.3 Séparation des fonctions

Lorsque des sphères de responsabilité sont conférées à certains rôles, les attributions et les responsabilités qui présentent un conflit doivent être attribuées à des rôles différents 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, lorsqu'ils ont trait à la gestion de la sécurité de l'information à l'Université, les conflits potentiels qui suivent doivent être assignés à des rôles différents ainsi qu'il est indiqué ci-dessous :

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 des comptes possédant des privilèges locaux élevés est documentée et approuvée par une ou un gestionnaire responsable approprié qui n'est pas autorisé à créer de tels comptes;

f) la création de comptes possédant des privilèges administratifs conférant un accès complet est documentée et approuvée par la ou le responsable de la sécurité de l'information, qui n'est pas autorisé à créer de tels comptes.

4.4 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 politiques 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 les politiques, normes et 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 des politiques, normes et procédures applicables;

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

5. Exceptions à la politique

5.1 Déclaration obligatoire en cas de non-conformité

Les actifs informationnels sensibles — quels qu'en soit la forme ou le propriétaire — doivent en tout temps être gérés en conformité avec les politiques, normes et exigences de l'Université, sans égard à la méthode ou à l'appareil employés 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 la sécurité de l'information; il ou elle signalera l'incident au Comité sur la sécurité de l'information, qui l'examinera 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.

5.2 Traitement des cas de non-conformité non autorisés

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 la sécurité 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;

b) restreindre l'accès physique aux zones sécurisées;

c) signaler les incidents aux ressources humaines.

6. Examens annuels et approbation des modifications

6.1 Examen annuel obligatoire

Le Comité sur la sécurité de l'information doit, avec la coordination du ou de la responsable de la sécurité de l'information, effectuer un examen formel des politiques du programme au moins une fois l'an. L'examen devrait notamment évaluer les possibilités d'amélioration à la suite de changements au sein de l'organisme, les exigences organisationnelles, les conditions juridiques, l'environnement technique et l'efficacité des mesures de sécurité.

6.2 Approbation des modifications

Les modifications proposées aux politiques du programme doivent toutes faire l'objet d'un examen formel par le Comité sur la sécurité de l'information. Après cet examen, ces modifications ne peuvent entrer en vigueur que lorsqu'elles ont été revues et approuvées par la rectrice ou le recteur (et approuvées par le Bureau des gouverneurs, lorsque son autorité prime sur celle de la rectrice ou du recteur).

6.3 Notification en cas de modification de la politique

Les modifications apportées à la politique et découlant de l'examen annuel seront communiquées dès que possible au personnel concerné. Les principales modifications seront intégrées à la formation offerte par l'Université au sujet des actifs informationnels sensibles.

7. Renvois

7.1 Politique sur la classification de l'information

7.2 Schéma de classification de l'information

7.3 Politique sur l'étiquetage et le traitement de l'information selon sa classification