CLASSIFICATION DE L'INFORMATION

(Procédure administrative)

Adoption
Date : CS 25/01/2023

Modifications
Date :

Ce document remplace tout règlement antérieur en cette matière.

Prochaine révision : 2028

SOMMAIRE

1. Énoncé de la procédure

Dans le cadre du programme de sécurité de l'information, la présente procédure souligne l'engagement et les exigences de l'Université de Saint-Boniface (ci-après « Université ») envers la protection des actifs informationnels sensibles contre l'accès, l'utilisation, la communication, l'interruption, la modification, l'inspection, l'enregistrement ou la destruction non autorisés au moyen de l'adoption d'un processus de classification des données à l'échelle de l'Université, lequel s'intègre dans la culture de cette dernière grâce à la formation et à un usage juste et raisonnable des pratiques et des activités de l'Université.

2. Champ d'application

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

3. Modalités de la procédure

La présente procédure s'applique à tous les actifs informationnels sensibles — quels qu'en soient la forme ou le ou la propriétaire — à l'échelle de l'Université, à toutes les personnes qui ont accès à ces actifs sensibles dans le cadre de leur emploi au sein de l'Université, de même qu'à l'ensemble des ressources, des appareils, des outils et des supports servant à cet accès.

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 **Comité sur la sécurité de l'information :** se compose des membres de l'équipe de direction (« propriétaires de l'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 le Service des installations et de la sécurité.

5. Responsabilités

5.1 Le vice-recteur ou la vice-rectrice à l'administration et aux finances est responsable du développement, de l'administration et de la révision de la présente procédure.

5.2 Le Comité sur la sécurité de l'information est responsable de concevoir et de gérer un système de classification de l'information, qui sera ensuite revu pour approbation par la rectrice ou le recteur.

6. Procédures

6.1 Classification obligatoire de l'information sensible

Les actifs informationnels sensibles qui sont obtenus, conservés, utilisés, transmis, archivés et détruits par l'Université doivent être classifiés afin d'assurer que ces activités soient conformes aux politiques, normes et procédures internes applicables de l'Université ainsi qu'aux exigences externes en matière de protection de l'information.

6.2 Inventaire de l'information

Les actifs informationnels sensibles qui ont été classifiés par l'Université doivent faire l'objet d'un suivi tout au long de leur cycle de vie au moyen d'un inventaire des actifs informationnels maintenu par le ou la responsable de l'information, comme défini dans la politique sur la Sécurité de l'information.

Les propriétaires de l'information, ou les usagers ou usagères qu'ils ou elles autorisent, doivent veiller à ce que les actifs informationnels sensibles nouvellement classifiés soient ajoutés à l'inventaire des actifs informationnels et à ce que les actifs désaffectés soient supprimés, soit directement, soit au moyen d'un processus approuvé de notification.

L'inventaire doit notamment comprendre ce qui suit :

a) le nom de l'actif (comme le nom du fichier ou du document);

b) une description de l'actif et de sa raison d'être;

c) le type d'actif informationnel (copie papier, fichier numérique, support ou dispositif portable, etc.);

d) des précisions sur l'actif, comme les étiquettes applicables en matière juridique ou règlementaire;

e) la date de rétention des données (ou les exigences, le cas échéant, y compris des renseignements historiques qui ne peuvent être détruits, mais qui doivent être archivés);

f) le niveau de sécurité, ou une note expliquant pourquoi un actif non classifié pourrait devenir sensible ultérieurement;

g) le ou la propriétaire de l'information;

h) la date du dernier examen des accès effectué par le ou la propriétaire de l'information;

i) l'emplacement approximatif de l'actif (unité ou numéro de salle, site externe d'entreposage, etc.);

j) tout manquement connu quant aux exigences en matière de contrôle, y compris les exceptions autorisées dont le besoin est démontré et consigné à l'écrit.

6.3 Système obligatoire de classification de l'information

Un système de classification de l'information doit être conçu et maintenu par le Comité sur la sécurité de l'information et tout changement devant y être apporté doit être approuvé par la rectrice ou le recteur.

Le système doit répondre aux critères suivants :

a) être élaboré au moyen d'un modèle de classification positive qui dirige les ressources principalement vers les actifs qui requièrent une protection et non vers ceux destinés à être communiqués ouvertement;

b) proposer au moins trois niveaux de sensibilité pour les actifs informationnels, ces niveaux étant fondés sur des critères comprenant minimalement l'incidence de toute perte ou divulgation non autorisée de l'actif;

c) respecter les exigences existantes prévues par la *Loi sur l'accès à l'information et la protection de la vie privée*, la *Loi sur les renseignements médicaux personnels* et la norme PCI DSS qui s'appliquent;

d) être actualisé au besoin lorsque ces exigences sont modifiées.

Le système de classification de l'information doit être communiqué à tous les usagers et usagères (dont le rôle est défini par la olitique sur la Sécurité de l'information) dont l'emploi nécessite un accès aux actifs informationnels sensibles contrôlés par l'Université.

6.4 Exigences en matière d'étiquetage et de traitement des actifs informationnels sensibles

Les exigences en matière d'étiquetage et de traitement de l'information sensible relatives à la classification de l'information doivent être communiquées à l'ensemble des usagers et usagères dont l'emploi nécessite un accès aux actifs informationnels sensibles gérés par l'Université. Les exigences devraient notamment couvrir les éléments suivants :

a) des directives en vue d'une classification uniforme et précise des actifs informationnels;

b) une norme en matière d'étiquetage employée de façon uniforme dans toute l'Université;

c) un procédé visant l'ajout et la suppression d'actifs informationnels sensibles au sein de l'inventaire des actifs maintenu par le ou la responsable de l'information;

d) des critères permettant d'accorder l'accès aux actifs informationnels sensibles, comme les fonctions des usagers, les principes de droit d'accès minimal et de la séparation des tâches ainsi que les ententes de confidentialité;

e) des exigences sur l'obtention, le stockage, l'utilisation, la transmission, la communication à des tiers (le cas échéant), le transport de même que l'archivage et la destruction d'information sensible lorsqu'elles ne sont pas prévues par les organismes de droit ou de règlementation.

6.5 **Accessibilité des exigences relatives au traitement et au système de classification de l'information**

Des versions à jour des exigences relatives au traitement et au système de classification de l'information ainsi qu'aux procédures connexes doivent être accessibles à tout le personnel de l'Université dont le travail comprend le traitement des actifs informationnels sensibles. Ces documents peuvent être disponibles en version électronique au moyen d'une structure de dossiers ou d'un portail Web sécurisés de façon appropriée.

6.6 **Signalement obligatoire des incidents concernant de l'information sensible**

a) Signalement obligatoire aux autorités appropriées

Les usagers et usagères doivent immédiatement aviser les propriétaires de l'information appropriés et le ou la responsable de l'information lorsqu'ils ou elles apprennent ou soupçonnent que de l'information sensible classifiée a été perdue ou encore traitée ou communiquée de façon inappropriée.

b) Enquête et recours hiérarchique en cas d'incident concernant de l'information sensible

Le ou la responsable de l'information doit enquêter sur les signalements de perte, de traitement ou de communication inappropriés d'information sensible. Si le signalement révèle un incident réel alors qu'aucune exception autorisée n'existe, les activités fautives doivent cesser immédiatement et l'incident, de même que les détails sur toute perte, communication ou autre conséquence, doivent être signalés dès que possible au ou à la responsable de l'information.

7. Renvois

7.1 *Loi sur l'accès à l'information et la protection de la vie privée*
7.2 *Loi sur les renseignements médicaux personnels*
7.3 Politique_Sécurité de l'information
7.4 Politique_Utilisation des services informatiques
7.5 Procédure_Contrôle de l'accès fondé sur la classification de l'information
7.6 Procédure_Étiquetage et le traitement de l'information classifiée
7.7 Procédure_Système de classification de l'information