SYSTÈME DE 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

La présente procédure énonce le système de classification de l'information adopté par l'Université de Saint-Boniface (ci-après « Université »), système de classification au sein duquel l'information est classifiée selon des niveaux de sécurité. Chaque niveau représente une criticité ou une valeur financière différente, ce qui entraine différentes exigences en matière de confidentialité, d'intégrité et de disponibilité. Les niveaux de sécurité permettent de fournir aux personnes qui traitent des informations sensibles des indications concises sur le traitement et la protection qui s'imposent.

2. Champ d'application

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

3. Modalités de la procédure

Le présent système de classification de l'information s'applique à la classification des actifs informationnels par les propriétaires de l'information compte tenu de leur valeur commerciale, de leur criticité et des exigences applicables découlant des organismes de droit ou de règlementation.

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 **Niveau confidentiel** : information devant être soigneusement contrôlée en raison des risques de préjudice envers l'Université, son personnel ou la population étudiante, ou information pour laquelle des lois ou des organismes de droit ou de règlementation exigent une protection élevée.

4.3 **Niveau interne** : information à laquelle une partie ou l'ensemble du personnel et de la population étudiante de l'Université ont accès, mais qui ne convient pas à la transmission à des parties intéressées externes telles que les médias ou le public général du site Web.

4.4 **Niveau non classifié** : information à laquelle tous les intervenants internes et externes peuvent accéder.

4.5 **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.

4.6 **Tiers** : une personne, un groupement ou une organisation autre que :
a) l'auteur de la demande;
b) un organisme public.

5. Responsabilités

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

5.2 La ou le responsable de l'information coordonne les activités du Comité de sécurité de l'information et lui sert de personne-ressource principale. Il ou elle travaillera de concert avec le Comité sur la sécurité de l'information afin de dresser l'inventaire des actifs informationnels de l'Université.

5.3 Le 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. Il désigne les propriétaires de l'information supplémentaire, recommande les exceptions aux procédures du programme et revoit les procédures du programme annuellement.

5.4 L'Université reconnait qu'elle a la responsabilité de se conformer aux lois et aux règlements fédéraux, provinciaux et municipaux pertinents. En cas d'incompatibilité entre les exigences en matière de classification, d'étiquetage et de traitement de l'information prévues par le présent système et celles des organismes de droit ou de règlementation pertinents, les exigences les plus strictes l'emportent, et, s'il y a lieu, le présent système sera revu et actualisé dans les meilleurs délais.

6. Procédures

6.1 Niveaux de sécurité pour la classification des données

Dans le cadre de la procédure sur le Système de classification de l'information, les trois niveaux de sécurité qui suivent s'appliquent aux actifs informationnels de l'Université, sans égard au propriétaire de l'information ni à la forme qu'ils revêtent.

6.1.1 Niveau non classifié

- **En voici des exemples :**
  - documents de marketing;
  - information d'ordre général affichée publiquement ou sur le site Web public;
  - information de recherche non personnelle et non exclusive;

- documents publiés pour usage public.

- **Étiquetage :** L'information non classifiée n'a pas à être étiquetée.

- **Gestion :** L'information non classifiée ne fait pas l'objet d'exigences particulières en matière de gestion.

- **Incidence :** Faible/mineure. La perte ou l'utilisation non autorisée d'information non classifiée entrainerait des conséquences très mineures, voire nulles, y compris les suivantes :
  - léger embarras en cas d'information inexacte ou périmée;
  - conséquences financières ou interruption commerciale nulles à faibles, comme la réimpression de documents ou la modification d'information sur un site Web.

- **Inventaire :** L'information non classifiée n'a pas à être répertoriée au sein de l'inventaire des actifs informationnels.

- **Traitement :** L'information non classifiée ne fait pas l'objet d'exigences particulières en matière de traitement.

6.1.2 **Niveau interne**

- **En voici des exemples :**
  - politiques et horaires internes;
  - documents de la bibliothèque ou documents archivés dont la circulation est restreinte;
  - portails Web internes;
  - information de recherche non personnelle, mais exclusive;
  - information exclusive reçue d'un fournisseur et visée par une entente de confidentialité;
  - listes mises à la disposition de tous les étudiants et étudiantes d'un cours ou d'un programme donné;
  - information concernant des affaires personnelles (naissances, décès, prises de retraite, etc.) communiquée par motif de compassion à une partie ou à l'ensemble de l'Université, mais pas au grand public;
  - autres informations pour lesquelles des lois ou des organismes de droit et de règlementation exigent une protection modérée.

- **Étiquetage :** L'information interne doit être étiquetée en conformité avec la procédure sur l'Étiquetage et le traitement de l'information classifiée de l'Université.

- **Gestion :** L'accès à l'information interne doit être géré en conformité avec la politique sur la gestion de l'Accès à l'information et respect de la vie privée de l'Université.

- **Incidence :** Moyenne/modérée. La perte ou l'utilisation non autorisée d'information interne entrainerait des conséquences indésirables, y compris les suivantes :
  - embarras ou malaise personnel pour un ou plusieurs particuliers, comme ce qui se produirait en cas de divulgation d'affaires personnelles;

- atteinte notable, mais gérable à la réputation ou aux activités de l'Université pouvant notamment nécessiter des excuses publiques ou donner lieu à de brèves interruptions;
- pertes financières notables, mais gérables, comme la perte d'occasions, de primauté de la publication ou d'accès à des journaux ou à d'autres documents protégés par des droits d'auteurs.

- **Inventaire :** L'information interne doit être répertoriée conformément aux exigences établies par la procédure sur la classification de l'information de l'Université; il doit notamment être clairement indiqué que cette information a été classifiée « interne ».

- **Traitement :** L'information interne doit être traitée en conformité avec les politiques et les procédures de l'Université en matière de traitement de l'information, comme celles portant sur l'étiquetage et le traitement de l'information, l'utilisation acceptable de l'information et la gestion de l'accès à l'information.

6.1.3 **Niveau confidentiel**

- **En voici des exemples :**
  - information permettant d'identifier une personne;
  - ébauche de convention collective pendant la négociation de celle-ci;
  - procès-verbal d'une rencontre où de l'information confidentielle a été abordée;
  - données financières sensibles;
  - information de recherche personnelle et exclusive;
  - notes et relevés des étudiants;
  - information sensible archivée;
  - autres informations pour lesquelles des lois ou des organismes de droit ou de règlementation exigent une protection élevée.

- **Incidence :** Élevée/importante. La perte ou l'utilisation non autorisée d'information confidentielle entrainerait des conséquences graves, y compris les suivantes :
  - préjudice grave à un ou à plusieurs particuliers notamment en cas de vol d'identité ou de divulgation de leur emplacement à des parties malveillantes;
  - atteinte grave à la réputation ou aux activités de l'Université, notamment la possibilité d'un scandale causé par la perte de données ou la fermeture d'un service en raison d'un incident lié à la sécurité ou à une enquête juridique;
  - pertes financières importantes, comme des amendes pour violation de la règlementation ou des dommages-intérêts découlant de poursuites.

- **Inventaire :** L'information confidentielle doit être répertoriée conformément aux exigences établies par la procédure sur la classification de l'information de l'Université; il doit notamment être clairement indiqué que cette information a été classifiée « confidentielle ».

- **Étiquetage :** L'information confidentielle doit être étiquetée en conformité avec la procédure sur l'étiquetage et le traitement de l'information de l'Université.

- **Traitement :** L'information confidentielle doit être traitée en conformité avec les politiques de l'Université en matière de traitement de l'information, comme celles

portant sur l'étiquetage et le traitement de l'information, l'utilisation acceptable de l'information et la gestion de l'accès à l'information.

- **Gestion :** L'accès à l'information confidentielle doit être géré en conformité avec la Politique sur la gestion de l'accès à l'information de l'Université.

6.2 Exigences en matière de protection de l'information des tiers

L'information d'un tiers à laquelle s'applique déjà un niveau de sécurité et qui est prêtée à l'Université en vue de son utilisation par cette dernière devrait se voir attribuer un niveau équivalent ou supérieur au sein du système de classification de l'Université et être conservée et traitée en conséquence. En voici des exemples :

a) les documents protégés par des droits d'auteur;
b) la propriété intellectuelle;
c) les documents de recherche classifiés.

6.3 Approche

L'Université emploie un modèle de classification positive où seules les informations jugées sensibles sont identifiées et classées selon les niveaux de sécurité.

Dans la classification d'un actif informationnel, il est tenu compte de sa criticité et de sa valeur en fonction du risque que présenterait sa perte ou sa mauvaise utilisation. Afin d'éviter des couts inutiles liés à la protection de l'information, le niveau de sécurité le plus faible qui puisse être raisonnablement envisagé devrait être accordé.

6.4 Inventaire des actifs potentiellement

L'inventaire des actifs informationnels est une composante essentielle du programme de sécurité de l'information et est établi selon les procédures ci-dessous.

a) Afin que la criticité et la valeur des actifs informationnels puissent être établies, et qu'on évalue ainsi leur nature sensible, ces actifs doivent faire l'objet d'un examen visant à déterminer le risque potentiel pour l'Université advenant leur perte ou leur divulgation ou utilisation non autorisée.
b) Tous les types d'information non sensible sont écartés, soit ceux dont la communication au public présenterait un risque faible, voire un effet potentiellement positif, sur l'Université, tels les documents de marketing, les documents publiés et les sites Web publics, lesquels peuvent demeurer non classifiés.
c) Créer des catégories pour certains types d'information au sein de l'inventaire. Ces catégories visent les actifs informationnels qui sont courants et de format constant, et qui peuvent par conséquent se faire attribuer un niveau de sécurité automatique fondé sur les critères associés à la catégorie.
d) Les actifs informationnels qui restent sont ensuite répertoriés à la pièce. Lorsqu'il est possible de le faire, il est plus efficace de grouper des données distinctes en un seul actif informationnel pouvant être traité en tant qu'unité logique unique. Les informations les plus sensibles employées à une fin donnée détermineront le niveau de sécurité accordé à toutes les informations connexes.
e) Les actifs informationnels de l'Université doivent être suivis tout au long de leur cycle de vie au moyen de l'inventaire des actifs informationnels que le ou la responsable de l'information tient et conserve.

6.5 **Procédure d'assignation de propriétaires de l'information aux actifs informationnels répertoriés**

Le Comité sur la sécurité de l'information revoit l'inventaire des actifs informationnels et affecte un ou une propriétaire de l'information à chaque actif informationnel répertorié.

6.6 **Procédure de classification des actifs informationnels répertoriés**

a) Les propriétaires de l'information examineront les actifs informationnels dont ils ont la responsabilité et définiront leur niveau de sécurité afin de veiller à ce qu'ils fassent l'objet des mesures de sécurité physiques et logiques appropriées. En définissant le niveau de sécurité, les propriétaires de l'information doivent tenir compte des éléments qui suivent :

- l'incidence potentielle en cas d'atteinte à la confidentialité, à l'intégrité ou à la disponibilité des actifs;
- le niveau de sécurité approprié, sachant que tout niveau trop élevé pourrait entrainer le recours à des procédures de sécurité inutiles (et à des couts inutiles) et que tout niveau trop faible pourrait mettre en danger la réalisation sécuritaire des objectifs institutionnels;
- dans certains cas, des informations agrégées peuvent être plus sensibles qu'un sous-ensemble d'informations ou que des informations individuelles.

b) L'accès à des actifs informationnels classifiés peut ensuite être autorisé ou révoqué en fonction des tâches liées à un poste et du niveau de sensibilité de l'information qui y est traitée.

- En créant une catégorie d'actifs informationnels nommée « documentation sur les configurations techniques », les propriétaires de l'information peuvent appliquer le niveau de sécurité « interne » à l'ensemble de la catégorie. Ainsi, tous les documents actuels ou futurs de ce type se verront automatiquement appliquer le niveau de sécurité « interne » sans devoir être classifiés à la pièce.
- En désignant des actifs informationnels individuels comme étant des « données du service de la paie », la ou le propriétaire de l'information peut y appliquer le niveau « confidentiel » et restreindre l'accès à une zone ou à une structure de dossiers données. La ou le propriétaire de l'information devra alors approuver chaque demande d'accès à cette zone ou à cette structure de dossiers.

6.7 **Modification du niveau de sécurité des actifs informationnels**

Un niveau de sécurité ne devrait s'appliquer à des informations que pendant la période où leur protection est nécessaire, après quoi un niveau inférieur devrait être défini ou elles devraient être déclassifiées. Les informations qui demeurent classifiées pendant toute leur durée de vie devraient être archivées ou détruites en conformité avec les exigences en matière de classification. Le niveau de sécurité peut être modifié au fil du temps.

Les propriétaires de l'information doivent tenir compte de ces éléments et revoir périodiquement les niveaux de sécurité qu'ils ont appliqués à leurs actifs informationnels.

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 ressources informatiques
7.5 Procédure_Classification de l'information
7.6 Procédure_ Contrôle de l'accès fondé sur la classification de l'information
7.7 Procédure_ Étiquetage et le traitement de l'information selon sa classification