ÉTIQUETAGE ET TRAITEMENT DE L'INFORMATION CLASSIFIÉE (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 les pratiques concernant l'étiquetage des actifs informationnels par les propriétaires de l'information et le traitement de ces actifs par les usagers ou usagères de l'Université de Saint-Boniface (ci-après « Université »), dont les rôles sont définis dans la politique sur la Sécurité de l'information. Conformément aux exigences énoncées dans les procédures de sécurité de l'information et de classification de l'information, tous les actifs informationnels classifiés doivent avoir des normes d'étiquetage et de manipulation pour garantir qu'ils soient traités de manière appropriée tout au long de leur cycle de vie.

2. Champ d'application

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

3. Modalité de la procédure

La présente procédure régit les méthodes d'étiquetage et de traitement visant à identifier la présence d'information sensible et à assurer la gestion sécuritaire des actifs informationnels jugés sensibles par les propriétaires de l'information à la suite de leur classification, dont les termes sont définis par le Système de classification de l'information.

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 **Cycle de vie :** décrit les différentes étapes de l'existence de documents depuis sa création ou sa réception jusqu'à sa disposition ou sa conservation à long terme à des fins historiques.

4.3 **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.

4.4 **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 du site Web.

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

4.6 **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.

4.7 **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.

4.8 **Zone de contrôle** : tous documents sous le contrôle du propriétaire de l'information

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 La ou le responsable de l'information est responsable d'offrir la formation en ce qui a trait à l'étiquetage et au traitement de l'information classifiée.

6. Procédures

6.1 Exigences en matière d'étiquetage et de traitement de l'information — niveau « non classifié »

L'étiquetage de l'information de niveau non classifié n'est pas nécessaire et aucune restriction visant l'accès ou le traitement de cette information n'est imposée pour des raisons de sécurité.

À la fin de son cycle de vie, l'information de niveau non classifié peut être détruite sans exigences particulières. L'information historique de niveau non classifié devrait plutôt être archivée.

6.2 Exigences en matière d'étiquetage et de traitement de l'information — niveau « interne »

Les exigences qui suivent s'appliquent à l'égard de l'étiquetage et du traitement de l'information de niveau interne.

6.2.1 Exigences en matière d'étiquetage de l'information

a) **Documents physiques (imprimés) conservés dans un dossier**

Lorsque des documents physiques (imprimés) sont conservés dans un contenant (comme un dossier), plusieurs documents peuvent s'y trouver. Dans un tel cas, étiquetez le dossier comme suit :

i. Indiquez le mot « INTERNE » pour noter le niveau d'information le plus sensible compris dans l'actif (même si certaines informations n'ont pas ce niveau).
ii. Indiquez le public cible du document, en forme abrégée.

b) **Documents de la suite Office (format papier ou électronique)**

Dans le cas des documents de niveau interne de la suite Office (comme les fichiers de traitement de texte, de chiffrier ou de présentation), le mot « INTERNE » doit figurer dans le nom du fichier et la mention « INTERNE » ainsi que le public cible doivent être indiqués dans l'entête du document ou en bas de page.

c) **Autres types d'information en format électronique**

i. Pour les fichiers électroniques qui ne proviennent pas de la suite Office, la mention « INTERNE » doit figurer dans le nom du fichier ou du dossier qui le contient, ou encore dans le nom de l'environnement de partage de fichiers.
ii. La ligne d'objet des courriels qui comportent de l'information de niveau interne doit porter la mention « INTERNE ».
iii. Lorsque l'information de niveau interne ne peut être étiquetée tel qu'il est indiqué ci-dessus, le ou la propriétaire de l'information doit concevoir un système d'étiquetage différent et en informer le ou la responsable de l'information.

6.2.2 Exigences en matière de traitement de l'information

a) **Autorisation et contrôles de sécurité**

Les propriétaires de l'information doivent explicitement autoriser les usagers et usagères, les groupes, les programmes et les facultés auxquels ils souhaitent accorder l'accès à de l'information interne au sein de leur zone de contrôle avant que cet accès ne puisse être accordé.

Les propriétaires de l'information doivent établir le public cible des actifs informationnels de niveau interne qui se trouvent au sein de leur zone de contrôle avant leur communication ou leur distribution par quelque moyen que ce soit.

Les usagers et usagères doivent veiller à ce que l'information de niveau interne dont l'accès leur a été accordé ne fasse l'objet d'aucune discussion ni communication auprès de personnes non autorisées (soit celles qui ne font pas partie du public cible établi par les propriétaires de l'information comme prévu ci-dessus).

Les usagers et usagères qui accèdent à de l'information de niveau interne ne doivent pas tenter de contourner les contrôles de sécurité prévus par la procédure sur le contrôle de l'accès et sont tenus de signaler au ou à la responsable de l'information tout défaut ou problème de configuration constaté ou soupçonné dans les contrôles de sécurité.

Les usagers et usagères doivent protéger les dispositifs d'accès, comme les clés, les cartes d'identité, les jetons électroniques et les mots de passe liés à des comptes qui offrent accès à de l'information de niveau interne ou à des endroits où cette information est conservée.

Les appareils personnels ne peuvent servir à photographier les actifs informationnels de niveau interne de l'Université.

b) **Supports de données portables**

Le stockage d'information de niveau interne sur un support de données portable doit être approuvé par le ou la propriétaire de l'information.

c) **Lorsque l'information n'est pas utilisée**

Lorsqu'ils ne sont pas utilisés, les dossiers physiques comprenant de l'information de niveau interne doivent être conservés de manière à ce que leur accès soit limité au personnel approprié, lorsque la distribution de l'information n'a pas encore été approuvée, ou au personnel et au public cible, lorsque sa distribution a eu lieu.

d) **Lorsque l'information est utilisée ou qu'elle fait activement l'objet d'un accès ou d'un transfert au sein de l'Université**

Les documents imprimés qui comportent de l'information de niveau interne doivent, dans la mesure du possible, être imprimés sur un dispositif dont l'accès est limité au personnel autorisé approprié; si le dispositif est partagé avec des personnes non autorisées, les documents doivent être récupérés sans délai.

L'information de niveau interne ne peut être saisie sur des sites Web ou d'autres services Internet à moins d'une autorisation du directeur ou de la directrice du Service des technologies de l'information.

Les courriels comportant de l'information de niveau interne doivent être distribués par l'entremise du service de courriel chiffré de l'Université et doivent être envoyés uniquement à des usagères et usagers autorisés.

Les usagers et usagères qui travaillent avec de l'information de niveau interne doivent verrouiller leur écran en tout temps lorsqu'ils et elles s'éloignent de leur poste de travail, à moins qu'une exception approuvée soit en vigueur.

Tout accès à distance à de l'information interne doit s'effectuer au moyen d'une méthode approuvée à cette fin par le directeur ou la directrice du Service des technologies de l'information.

e) **Lorsque des fichiers physiques ou des supports de données portables sont transportés ou retirés de zones sécurisées**

Les exigences qui suivent s'appliquent aux fichiers et aux supports de données physiques comportant de l'information de niveau interne qui sont transportés ou retirés de zones sécurisées :

i. lorsqu'ils sont envoyés à un site externe pour stockage (pour qu'on effectue des copies de sauvegarde, par exemple), ils doivent être conservés dans des contenants marqués « INTERNE » dans un endroit dont l'accès est limité aux personnes possédant les autorisations appropriées;
ii. lorsqu'ils sont retirés de l'Université à l'intention d'un ou d'une destinataire externe, ils doivent faire l'objet d'une permission documentée expresse de la part du ou de la propriétaire de l'information;

iii. lorsque les supports de données physiques (y compris les fichiers physiques et les documents imprimés) qui comprennent de l'information de niveau interne sont transportés à l'intention d'une ou d'un destinataire externe autorisé, ils doivent :
- être chiffrés, si le fichier se trouve sur un support physique de stockage électronique;
- être scellés dans un contenant qui indique qu'ils sont sensibles et qui permettrait de constater toute altération;
- être envoyés par l'entremise d'un messager ou d'une messagère digne de confiance ou par courrier recommandé.

f) **Lorsque l'information est recueillie initialement**

Toute nouvelle information doit être classifiée et étiquetée de niveau interne dès que possible.

g) **Lorsque l'information a atteint la fin de son cycle de vie**

L'information de niveau interne qui arrive à la fin de son cycle de vie et qui n'est pas de nature historique doit être détruite avant d'être éliminée. Les dispositifs servant à stocker de l'information de niveau interne doivent être effacés de façon sure avant d'être vendus, donnés ou utilisés à une autre fin.

L'information de niveau interne de nature historique ne peut être détruite et doit plutôt être archivée; son accès doit être limité au personnel autorisé approprié.

6.3 **Exigences en matière d'étiquetage et de traitement de l'information — niveau « confidentiel »**

Les exigences qui suivent s'appliquent à l'égard de l'étiquetage et du traitement de l'information de niveau confidentiel.

6.3.1 Exigences en matière d'étiquetage de l'information

a) **Documents physiques (imprimés) conservés dans un dossier**

Lorsque des documents physiques (imprimés) sont conservés dans un contenant (comme un dossier), plusieurs documents peuvent s'y trouver. Dans un tel cas, étiquetez le dossier comme suit :

i. Indiquez le mot « CONFIDENTIEL » pour noter le niveau d'information le plus sensible compris dans l'actif (même si certaines informations n'ont pas ce niveau).
ii. Indiquez le titre du ou de la propriétaire de l'information :
iii. il n'est pas nécessaire d'indiquer le public cible puisque l'accès est accordé explicitement à des usagères et usagers donnés par le ou la propriétaire de l'information, mais le titre de ce dernier ou de cette dernière peut servir à obtenir de l'information ou à lui signaler que de l'information de niveau confidentiel a été trouvée à un endroit inapproprié).

b) **Documents de la suite Office (format papier ou électronique)**

Dans le cas des documents de niveau confidentiel de la suite Office (comme les fichiers de traitement de texte, de chiffrier ou de présentation), la mention « CONFIDENTIEL » doit figurer dans le nom du fichier et la mention

« CONFIDENTIEL » ainsi que le titre du ou de la propriétaire de l'information doivent être indiqués dans l'entête du document ou en bas de page.

c) **Autres types d'informations en format électronique :**

i. Pour les fichiers électroniques qui ne proviennent pas de la suite Office, la mention « CONFIDENTIEL » doit figurer dans le nom du fichier ou du dossier qui le contient, ou encore dans le nom de l'environnement de partage des fichiers.
ii. La ligne d'objet des courriels qui comportent de l'information de niveau confidentiel doit porter la mention « CONFIDENTIEL ».
iii. Lorsque l'information confidentielle ne peut être étiquetée tel qu'il est indiqué ci-dessus, le ou la propriétaire de l'information doit concevoir un système d'étiquetage différent et en informer le ou la responsable de l'information.

6.3.2 Exigences en matière de traitement de l'information

a) **Autorisation et contrôles de sécurité**

Les propriétaires de l'information doivent explicitement autoriser les usagères et usagers individuels qu'ils ou elles souhaitent ajouter aux groupes d'usagers ayant accès à de l'information de niveau confidentiel au sein de leur zone de contrôle avant que cet accès ne leur soit accordé.

Les propriétaires de l'information doivent suivre les usagers et usagères et leur rôle au sein des groupes d'usagers dont l'accès à de l'information de niveau confidentiel est autorisé au sein de leur zone de contrôle.

Les usagères et usagers autorisés à accéder à de l'information de niveau confidentiel doivent signer une entente de non-divulgation avant que l'accès ne leur soit accordé.

Les demandes d'accès à l'information de niveau confidentiel d'un particulier ou d'une particulière en lien avec l'Université provenant de tiers doivent être évaluées attentivement par les propriétaires de l'information afin de s'assurer que les exigences qui sont en vigueur au moment de la demande et qui proviennent d'organismes juridiques ou règlementaires soient respectées avant la communication de l'information, en suivant les conseils de la coordination de la protection de la vie privée.

Les propriétaires de l'information doivent établir le public cible des actifs informationnels confidentiels qui se trouvent au sein de leur zone de contrôle avant leur communication ou leur distribution par quelque moyen que ce soit.

Les usagers et usagères doivent veiller à ce que l'information de niveau confidentiel dont l'accès leur a été accordé ne fasse l'objet d'aucune discussion ni communication auprès de personnes non autorisées (soit celles qui ne font pas partie des usagères et usagers autorisés établis par les propriétaires de l'information comme prévu ci-dessus).

Les usagers et usagères qui accèdent à de l'information de niveau confidentiel ne doivent pas tenter de contourner les contrôles de sécurité prévus par la procédure sur le contrôle de l'accès et sont tenus de signaler au ou à la responsable de

l'information tout défaut ou problème de configuration constaté ou soupçonné dans les contrôles de sécurité.

Comme le prévoit la politique touchant l'Utilisation des ressources informatiques, les usagers et usagères doivent protéger les dispositifs d'accès, comme les clés, les cartes d'identité, les jetons électroniques et les mots de passe liés à des comptes qui donnent accès à de l'information de niveau confidentiel ou à des endroits où cette information est conservée.

Les appareils personnels ne peuvent servir à photographier les actifs informationnels de niveau confidentiel de l'Université.

b) **Supports de données portables**

Le stockage d'information de niveau confidentiel sur un support de données portable doit être approuvé par le ou la propriétaire de l'information et employer un mode de chiffrage approuvé par le Service des technologies de l'information, et le ou la responsable de l'information doit porter à l'inventaire le support de données et son contenu.

c) **Lorsque l'information n'est pas utilisée**

Les dossiers physiques comprenant de l'information de niveau confidentiel doivent être conservés dans une pièce ou un contenant verrouillé, comme un tiroir ou un classeur, et leur accès doit être limité au seul personnel autorisé.

d) **Lorsque l'information est utilisée ou qu'elle fait activement l'objet d'un accès ou d'un transfert au sein de l'Université**

Les documents imprimés qui comportent de l'information de niveau confidentiel doivent, dans la mesure du possible, être imprimés sur un dispositif dont l'accès est limité au personnel autorisé approprié; si le dispositif est partagé avec des personnes non autorisées, les documents doivent être récupérés sans délai.

L'information de niveau confidentiel ne peut être saisie sur des sites Web ou d'autres services Internet à moins d'une autorisation du directeur ou de la directrice du Service des technologies de l'information.

Les courriels comportant de l'information de niveau confidentiel doivent être distribués par l'entremise du service de courriel chiffré de l'Université et doivent être envoyés uniquement aux usagères et usagers autorisés.

Les usagers et usagères qui travaillent avec de l'information de niveau confidentiel doivent verrouiller leur écran en tout temps lorsqu'ils ou elles s'éloignent de leur poste de travail, à moins qu'une exception approuvée ne soit en vigueur.

Tout accès à distance à de l'information de niveau confidentiel doit être limité aux usagères et usagers autorisés par le ou la propriétaire de l'information et s'effectuer au moyen d'une méthode approuvée à cette fin par le directeur ou la directrice du Service des technologies de l'information.

e) **Lorsque des fichiers ou des supports de données physiques sont transportés ou retirés de zones sécurisées**

L'information de niveau confidentiel devant être retirée de l'unité ne peut quitter la zone qu'avec la signature de l'usagère ou l'usager autorisé et doit être rapportée sans délai dès que son utilisation prévue est terminée.

L'information de niveau confidentiel qui est retirée de l'Université à l'intention d'un ou d'une destinataire externe doit faire l'objet d'une permission documentée expresse de la part du ou de la propriétaire de l'information.

Les fichiers et les supports de données physiques comportant de l'information de niveau confidentiel qui sont envoyés à un site externe pour stockage (pour qu'on effectue des copies de sauvegarde, par exemple) doivent être conservés dans des contenants marqués « CONFIDENTIEL » dans un endroit dont l'accès est limité aux personnes possédant les autorisations appropriées.

Les supports de données physiques (y compris les documents imprimés et le support de stockage électronique) qui contiennent de l'information de niveau confidentiel et qui sont transportés vers un contenant externe autorisé doivent faire l'objet d'une permission documentée expresse de la part du ou de la propriétaire de l'information et doivent, durant le transport :

i. être chiffrés, si le fichier se trouve sur un support physique de stockage électronique;
ii. être documentés de façon à ce que l'autorisation du propriétaire de l'information, le contenu, l'expéditeur, la ou le destinataire prévu, la date et le mode d'envoi ainsi que le numéro de suivi soient accessibles au ou à la propriétaire de l'information et au ou à la responsable de l'information;
iii. être scellés dans un contenant qui indique qu'ils sont sensibles et qui permettrait de constater toute altération;
iv. être envoyés par l'entremise d'un messager ou d'une messagère digne de confiance ou par courrier recommandé;
v. faire l'objet d'une signature lorsque la ou le destinataire prévu les reçoit.

f) **Lorsque l'information est recueillie initialement**

Toute nouvelle information doit être classifiée et étiquetée de niveau confidentiel dès que possible.

L'information de niveau confidentiel doit être recueillie de façon à prévenir que des personnes non autorisées entendent ou voient l'information obtenue.

L'acquisition d'information de niveau confidentiel de même de son accès doivent être conformes à la *Loi sur l'accès à l'information et la protection de la vie privée* et aux autres exigences en matière juridique ou règlementaire :

i. le personnel de l'Université responsable de la collecte d'information de niveau confidentiel doit recevoir une formation lui permettant d'expliquer la raison ou le but de la collecte d'information sensible et de connaitre les exigences qui proviennent d'organismes juridiques ou règlementaires et qui s'appliquent à l'information obtenue;
ii. la collecte d'information de niveau confidentiel doit s'effectuer de manière à assurer la vérification de l'identité de la personne qui les fournit (et de ses parents ou tuteurs, lorsque la loi l'exige);
iii. les particuliers et les particulières (y compris les anciens étudiants et étudiantes, et les anciens membres du personnel) peuvent consulter ou modifier les renseignements personnels qui les concernent et peuvent en

demander des copies (nom, adresse, numéro de téléphone, etc.), mais uniquement par des moyens autorisés par le ou la propriétaire de l'information, notamment en personne avec une pièce d'identité ou par l'entremise d'un portail Web chiffré doté d'authentification à facteurs multiples; les méthodes d'accès électroniques doivent être approuvées et supportées par le Service des technologies de l'information;

iv. les notes des étudiants et étudiantes et la documentation connexe doivent être gérées en conformité avec les procédés établis par les propriétaires de l'information appropriés.

g) **Lorsque l'information a atteint la fin de son cycle de vie**

L'information de niveau confidentiel qui arrive à la fin de son cycle de vie et qui n'est pas de nature historique doit être détruite avant d'être éliminée. Les dispositifs servant à stocker de l'information de niveau confidentiel doivent être effacés de façon sure avant d'être vendus, donnés ou utilisés à une autre fin. Du personnel qualifié doit confirmer que les données ont été effacées de façon sure (selon les directives du directeur ou de la directrice du Service des technologies de l'information); la personne qui effectue la procédure ne peut être celle qui confirme qu'elle a été effectuée.

L'information de niveau confidentiel de nature historique ne peut être détruite et doit plutôt être archivée; son accès doit être limité au personnel autorisé approprié.

6.4 **Exceptions à la procédure**

6.4.1 Exigences quant à l'approbation des exceptions

Lorsque les procédures liées à la classification de l'information nuisent aux activités opérationnelles essentielles, les demandes d'exception doivent passer par le ou la propriétaire de l'information, comme le prévoit en détail la Politique sur la sécurité de l'information, et ces exceptions ne peuvent être mises en œuvre tant qu'une permission documentée n'a pas été obtenue de la part du ou de la propriétaire de l'information.

6.4.2 Exception visant les présentations

Dès l'approbation de la présente procédure, une exception à la règle voulant que les appareils et les postes de travail soient automatiquement verrouillés est accordée aux membres du personnel de soutien et du corps professoral lorsqu'ils donnent des présentations. Les présentateurs ou présentatrices doivent plutôt veiller à ce que les documents électroniques qui contiennent de l'information interne ou confidentielle qui ne fait pas partie de la présentation soient fermés lorsqu'un appareil ou un poste de travail est utilisé à cette fin.

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_ Système de classification de l'information