# CONTRÔLE DE L'ACCÈS FONDÉ SUR LA 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 les contrôles et les pratiques qui protègent la confidentialité, l'intégrité et la disponibilité des actifs informationnels sensibles de l'Université de Saint-Boniface (ci-après « Université »). En plus d'appuyer les autres politiques et procédures mises en place dans le cadre du programme de sécurité de l'information, cette procédure établit les règles quant à l'accès à l'information, aux systèmes, à l'équipement et aux installations ayant diverses classifications. Elle définit les responsabilités, conditions et pratiques spécifiques conçues pour protéger les actifs informationnels sensibles tout en soutenant les valeurs de l'Université, soit d'être un endroit ouvert et accueillant où l'on peut travailler, étudier, enseigner, collaborer et faire de la recherche.

## 2. Champ d'application

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

## 3. Modalités de la procédure

3.1 La présente procédure s'applique aux actifs informationnels classifiés de l'Université, quels qu'en soient la forme ou le ou la propriétaire, aux personnes qui y accèdent dans le cadre de leur emploi au sein de l'Université ainsi qu'à l'ensemble des ressources, appareils, outils et supports servant à la conservation, à l'accès, à l'utilisation et à la destruction de tels actifs. Les personnes qui accèdent au réseau wifi public de l'Université ne sont pas visées par la présente procédure.

3.2 Selon la procédure sur la Classification de l'information, les contrôles de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité de l'information et des systèmes d'information doivent

être établis de façon appropriée compte tenu de leur niveau de sécurité. Les propriétaires de l'information, au moyen du processus de classification de sécurité, déterminent les contrôles d'accès qui sont appropriés et qui doivent être appliqués à l'information sensible et aux systèmes d'information au moyen de cette classification.

## 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 **Mot de passe** : Le terme « mot de passe » s'entend à la fois au sens de mots de passe et de phrases passe.

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 **Zone sécurisée :** zones désignées par les propriétaires de l'information comme des zones sensibles appropriées pour la conservation des actifs informationnels de niveau confidentiel ou interne et qui sont sous leur contrôle.

## 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 Le ou la responsable de l'information doit évaluer, au moins une fois par année, l'efficacité des contrôles d'accès physique qui sont en place dans les zones sécurisées.

5.3 Le ou la responsable de l'information doit périodiquement auditer les droits d'accès des usagers et usagères pour veiller à ce qu'elles soient exécutées correctement.

## 6. Procédures

### 6.1 Contrôles d'accès physique dans les zones sécurisées

#### 6.1.1 Identification de « zone sécurisée »

Les zones sécurisées font l'objet d'un suivi au sein de l'inventaire des actifs informationnels de sorte que les propriétaires de l'information et le ou la responsable de l'information connaissent tous les endroits où l'information de niveaux confidentiel et interne est conservée ou utilisée et ceux où l'on peut y avoir accès.

Lorsqu'une zone a été désignée sécurisée, son périmètre de sécurité doit être défini et les contrôles physiques de sécurité doivent être appliqués.

6.1.2 Contrôles d'accès physique

Les zones sécurisées doivent être protégées par une barrière de sécurité physique ininterrompue et jumelée à des contrôles d'accès physique visant à prévenir l'accès non autorisé, leur conception pouvant varier d'une zone sécurisée à l'autre et devant être documentée par le ou la responsable de l'information. Les exigences minimales en matière d'accès physique sont les suivantes :

a) les portes d'accès doivent être munies de dispositifs d'accès électroniques, de verrous sécuritaires à clé ou à combinaison, selon ce qui s'avère approprié, qui sont installés et entretenus par l'équipe du Service des installations et de la sécurité;
b) l'accès doit être limité au personnel autorisé par la ou le propriétaire de l'information approprié;
c) la distribution des dispositifs de contrôle d'accès physique sera autorisée par les propriétaires de l'information, et leur gestion et leur mise en œuvre se feront en conformité avec les pratiques normatives du Service des ressources humaines, du Service des technologies de l'information et du Service des installations et de la sécurité;
d) les dispositifs de contrôle d'accès physique doivent être approuvés, installés, gérés, retirés et remplacés exclusivement par le Service des installations et de la sécurité.

En cas d'incompatibilité entre la présente procédure et la règlementation en matière d'incendies et de sécurité, cette dernière l'emporte et la présente procédure sera actualisée dans les meilleurs délais.

6.1.3 Travail dans les zones sécurisées

Le personnel qui travaille dans les zones sécurisées doit respecter les consignes suivantes :

a) traiter et sécuriser l'information classifiée en conformité avec la procédure sur l'étiquetage et le traitement de l'information classifiée;
b) maintenir la confidentialité des activités relatives à l'information classifiée qui se déroulent dans la zone sécurisée;
c) ne pas utiliser d'équipement d'enregistrement photographique, vidéo, audio ou autre sans l'autorisation du ou de la propriétaire de l'information;
d) veiller à ce que l'accès soit physiquement verrouillé avant de quitter la zone lorsqu'aucun personnel autorisé n'y est présent;
e) ne pas permettre à des visiteurs ou visiteuses non accompagnées d'être dans la zone sécurisée.

Note : Les entrepreneurs d'entretien ou de réparation doivent demander une autorisation visant une fin précise, selon la nécessité de la situation, et travailler sous la supervision du superviseur ou de la superviseure des opérations de l'Université. Ces demandes, et les approbations éventuelles, doivent être consignées à l'écrit.

6.1.4 Conservation physique de l'information sensible

Lorsque l'information de niveau confidentiel ou interne est conservée dans une zone sécurisée, elle doit également être conservée dans une filière, un tiroir ou un autre contenant semblable qui peut être verrouillé et doit être sous verrou lorsque la zone n'est pas occupée par au moins une personne autorisée à accéder à cette information.

6.1.5 Évaluation continue des zones sécurisées

Le ou la responsable de l'information doit évaluer, au moins une fois par année, l'efficacité des contrôles d'accès physique qui sont en place dans les zones sécurisées.

Tout signalement voulant qu'un contrôle d'accès physique n'aurait pas fonctionné comme défini et prévu, ou aurait été modifié ou laissé désactivé ou déverrouillé intentionnellement (selon ce que détermine le ou la propriétaire de l'information) doit faire l'objet d'une analyse des causes fondamentales et le directeur ou la directrice du Service des installations et de la sécurité doit entreprendre des mesures correctives. Ces incidents, de même que toute mesure corrective éventuelle, doivent être consignés à l'écrit et la documentation pertinente doit être communiquée au ou à la responsable de l'information.

## 6.2 Contrôles d'accès logique

6.2.1 Identificateurs d'utilisateur

L'accès aux réseaux, aux services réseau et aux systèmes d'information doit être autorisé, géré, suivi et contrôlé en fonction des besoins institutionnels et des exigences en matière de sécurité. L'accès à toute information possédant un niveau de sécurité autre que « non classifié » doit répondre aux principes de sécurité généraux du « besoin de connaitre » et du « droit minimal d'accès » et l'accès des usagers et usagères doit être expressément autorisé comme suit :

a) **Niveau non classifié :**
L'accès peut être fourni de manière anonyme à « tous les usagers », à « toutes les adresses IP » ou aux deux. Si une forme d'authentification est exigée, seuls les identificateurs d'utilisateur valides et fournis par l'Université sont autorisés.

b) **Niveau interne :**
L'accès requiert un identificateur d'utilisateur valide et fourni par l'Université.

c) **Niveau confidentiel :**
L'accès requiert un identificateur d'utilisateur valide et fourni par l'Université. L'attribution de l'accès à l'identificateur d'utilisateur nécessite l'approbation expresse du ou de la propriétaire de l'information.

6.2.2 Accès au réseau et à la zone réseau

L'accès au périmètre logique de sécurité de l'Université, ou à des zones réseaux particulières situées dans ce périmètre, peut également être limité à certains types d'accès réseau, selon le niveau de sécurité du système en question :

a) **Niveau non classifié :**
Toutes les formes d'accès réseau sont permises, y compris à partir d'Internet.

b) **Niveau interne :**
L'accès au réseau doit provenir de l'intérieur du périmètre logique de sécurité de l'Université, y compris par l'entremise de solutions de réseau privé virtuel (RPV) approuvées.

c) **Niveau confidentiel :**

i. L'accès réseau doit provenir de l'intérieur du périmètre logique de sécurité de l'Université, y compris par l'entremise de solutions de RPV approuvées.
ii. Chaque zone réseau conçue pour contenir des services réseau ou de l'information de niveau confidentiel doit constituer un sous-réseau de

protocole Internet distinct, et des listes de contrôle d'accès par pare-feu ou basées sur l'adresse IP et le port d'accès doivent être employées afin de limiter l'accès des usagers et usagères à la zone aux seuls cas justifiés par des besoins opérationnels légitimes. Les exceptions au modèle du droit minimal d'accès doivent, en sus du processus habituel, être approuvées par le ou la propriétaire de l'information.

iii. Des systèmes de détection ou, préférablement, de prévention des intrusions avec surveillance doivent être en place soit au périmètre logique de la zone, soit sur l'hôte même.

6.2.3 Obligation de contrôler l'emplacement des systèmes d'information qui hébergent de l'information électronique sensible

Les emplacements physiques autorisés en vue d'héberger de l'information électronique sont contrôlés en fonction du niveau de sécurité du système en question :

a) **Niveau non classifié :**
Les systèmes d'information qui stockent la copie de référence de l'information de niveau non classifié doivent être situés dans une zone sécurisée approuvée.

b) **Niveau interne :**
Les systèmes d'information qui stockent de l'information de niveau interne doivent être situés dans une zone sécurisée approuvée.

c) **Niveau confidentiel :**
Les systèmes d'information qui stockent de l'information de niveau confidentiel doivent être situés dans une zone sécurisée approuvée et desservir uniquement la zone réseau appropriée en conformité avec des règles pare-feu limitant l'accès au sous-réseau de la zone sécurisée ou au moyen de contrôles équivalents.

6.2.4 Obligation de protéger les copies de sauvegarde

Des contrôles doivent être en place pour protéger les copies de sécurité qui comprennent de l'information confidentielle contre l'interception, la divulgation, la modification ou les dommages pendant le transport :

a) **Niveau non classifié ou interne :**
Les copies de sauvegarde d'information de niveau non classifiée ou interne doivent être maintenues et conservées hors site afin de permettre leur restauration et d'aider à assurer leur disponibilité.

b) **Niveau confidentiel :**
Les supports de copies de sauvegarde doivent être protégés contre tout accès non autorisé d'une façon approuvée (tel le chiffrage) par le ou la responsable de l'information, puis transportés et conservés de façon sécuritaire hors site.

6.2.5 Obligation de protéger les systèmes d'information contre les logiciels malveillants

Puisque les logiciels malveillants peuvent affecter la disponibilité ou l'intégrité de l'information, ou fournir à des acteurs pernicieux un accès non autorisé et compromettre leur confidentialité, les actifs informatiques qui hébergent de l'information classifiée ou qui y accèdent doivent être protégés selon les normes minimales qui suivent :

a) **Niveau non classifié :**
Les systèmes d'information qui hébergent de l'information de niveau non classifié doivent utiliser des logiciels antivirus à jour qui sont munis de signatures courantes et qui sont configurés par le Service des technologies de l'information pour effectuer une recherche de virus périodique.

b) **Niveau interne :**
Les systèmes d'information qui hébergent de l'information de niveau interne doivent utiliser des logiciels antivirus à jour, être configurés pour effectuer une recherche de virus périodique, ainsi qu'une recherche au moment de l'accès si la performance le permet, et être administrés et surveillés centralement par le Service des technologies de l'information.

c) **Niveau confidentiel :**
Les systèmes d'information qui hébergent de l'information de niveau confidentiel ou qui y accèdent doivent utiliser des logiciels antivirus à jour qui sont configurés pour effectuer une recherche périodique et au moment de l'accès, et être administrés et surveillés centralement par le Service des technologies de l'information.

## 6.3 Identificateurs d'utilisateur — enregistrement, révocation, provisionnement et renseignements secrets d'authentification

6.3.1 Équivalence obligatoire

Afin de prévenir tout accès non autorisé aux systèmes et aux applications, les systèmes et les applications qui utilisent des identificateurs d'utilisateur locaux et internes (tirés d'une base de données, par exemple) plutôt que de faire appel à un système central d'authentification doivent gérer et surveiller les identificateurs de façon équivalente ou supérieure aux méthodes employées à l'égard des identificateurs centraux.

Lorsque le système ou l'application offre des capacités de contrôle supplémentaires, un usage approprié de ces contrôles doit être envisagé et mis en place selon le principe de sécurité général du droit minimal d'accès.

6.3.2 Exigences applicables à la création d'identificateurs d'utilisateur

Avant que les identificateurs d'utilisateur soient créés, et avant que l'accès à tout système d'information leur soit accordé, ils doivent être validés afin d'assurer :

a) qu'ils sont uniques et que la personne qui en est propriétaire est défini — dans le cas d'un compte de service, cette personne doit être celle qui occupe le rôle de responsable du service;
b) qu'il ne s'agit pas d'un identificateur d'utilisateur partagé ou d'invité, lequel n'est pas permis.

6.3.3 Surveillance des comptes privilégiés ou de service

Les comptes dont les privilèges sont globaux, de même que les comptes de service, doivent être consignés dans une liste centralisée des comptes sensibles; le ou la responsable de l'information doit avoir accès à cette liste à des fins d'audit.

6.3.4 Exigences relatives aux comptes de service

Les comptes de service, soit les identificateurs d'utilisateur privilégiés spéciaux qui sont utilisés par des applications, des systèmes ou des services plutôt que par des usagers ou usagères, doivent souvent avoir des mots de passe qui n'expirent pas automatiquement et qui ne se verrouillent pas après plusieurs tentatives de connexion ratées puisque le service qu'ils servent doit continuer à fonctionner.

Pour remplir ce besoin, des exigences supplémentaires sont imposées à leur égard :

a) ils doivent être approuvés par la direction du Service des technologies de l'information;
b) ils ne peuvent permettre des tentatives de connexion interactives, de sorte que le personnel ne puisse pas saisir le nom d'usager et le mot de passe du compte afin accéder de façon interactive aux ressources du réseau et du domaine dans l'environnement;
c) ils seront utilisés pour un service ou une fonction précise ou discrète et ne pourront être réutilisés pour plusieurs services ou fonctions;
d) ils doivent être configurés selon le principe du droit d'accès minimal leur permettant de remplir leur rôle ou fonction définis;
e) leur configuration ne permet pas l'accès à distance ou par RVP;
f) leur mot de passe doit être généré aléatoirement et répondre aux exigences de complexité minimales établies par la direction du Service des technologies de l'information;
g) leur mot de passe est fourni seulement au personnel approprié selon le principe de l'accès sélectif au moment de l'enregistrement ou de l'ajout de tâches à un service de tâches automatisées et ne peut être communiqué à des personnes non autorisées;
h) il faut mettre en place une surveillance des cas de multiples tentatives de connexion échouées.

6.3.5 Identificateurs d'utilisateur dont l'usage cesse temporairement

L'accès des usagers ou usagères qui s'absentent pour un congé peut être désactivé pendant toute la durée de leur absence.

6.3.6 Identificateurs d'utilisateur dont l'usage n'est plus requis

En cas de cessation d'emploi, les identificateurs d'utilisateur doivent immédiatement être désactivés, les permissions doivent être retirées et le mot de passe doit être changé. Les identificateurs peuvent être supprimés à une date ultérieure lorsque les exigences en matière de planification de transition et de rétention des données le permettront.

En cas de cessation d'emploi irrégulière ou pour des raisons de sécurité, le compte désactivé doit être revu par le Service des technologies de l'information dans les 24 heures qui suivent pour établir s'il y a eu des activités irrégulières ou suspectes.

6.3.7 Provisionnement d'accès aux usagers

Un processus formel de provisionnement d'accès aux usagers et usagères doit être mis en place en vue d'attribuer ou de révoquer des droits d'accès de tous les types d'usagers à tous les systèmes et services. Ce processus doit notamment :

a) obtenir l'approbation d'une autorité prédéterminée et, dans le cas d'un accès confidentiel, du ou de la propriétaire de l'information;

b) veiller à ce que les droits d'accès ne soient pas activés avant que l'approbation ne soit accordée;
c) comporter une étape de vérification pour confirmer que la demande d'accès répond au principe de sécurité de base de la séparation des tâches;
d) maintenir des dossiers centralisés sur les droits d'accès accordés à chaque identificateur d'utilisateur;
e) prévenir le provisionnement par duplication des accès;
f) si possible, favoriser l'accès basé sur les rôles.

6.3.8 Gestion des droits d'accès privilégiés

Pour l'application de la présente procédure, les droits d'accès privilégiés s'entendent au sens de la capacité d'un compte d'outrepasser une partie ou la totalité des contrôles de sécurité.

Afin de prévenir l'usage inapproprié des droits d'accès privilégiés, la gestion de ces droits comprend des exigences supplémentaires qui doivent, au minimum, assurer ce qui suit :

a) les droits d'accès privilégiés sont attribués à un identificateur d'utilisateur différent de l'identificateur ordinaire servant aux activités opérationnelles régulières, lesquelles ne peuvent être effectuées à partir de l'identificateur privilégié;
b) les identificateurs d'utilisateur génériques ne sont pas permis;
c) l'accès privilégié est accordé uniquement si cela est nécessaire pour accomplir le travail exigé;
d) les demandes de service en vue de l'obtention de droits d'accès privilégiés sont approuvées par la ou le propriétaire de l'information approprié.

Les usagers et usagères qui possèdent des droits d'accès privilégiés doivent répondre à d'autres exigences :

a) ils doivent avoir reçu une formation de sensibilisation à la sécurité avant de recevoir les authentifiants relatifs au compte doté de droits d'accès privilégiés;
b) la divulgation ou le partage des authentifiants pour les comptes dotés de droits d'accès privilégiés est strictement interdite.

L'activité des usagères ou usagers privilégiés doit être consignée à un endroit auquel ne peuvent accéder les usagers ou usagères qui font l'objet d'une surveillance (p. ex. au moyen d'une vérification par une tierce partie ou de registres où seuls les ajouts sont possibles).

6.3.9 Gestion des renseignements secrets d'authentification

La gestion des renseignements secrets d'authentification (mots de passe, etc.) doit s'effectuer au moyen d'un processus formel permettant notamment d'assurer ce qui suit :

a) lorsqu'un nouvel identificateur d'utilisateur est fourni, ou qu'un mot de passe est réinitialisé, un mot de passe temporaire et aléatoire est attribué et fourni à l'usager ou l'usagère, qui doit changer son mot de passe à la première utilisation;
b) le mot de passe temporaire doit être fourni à l'usager ou l'usagère de façon sécuritaire, notamment hors ligne (par ex. par téléphone) ou en ligne de façon chiffrée (par ex. un service de messagerie sécurisé) et toute transmission en texte non chiffré est interdite;
c) le déverrouillage d'un identificateur d'utilisateur exige une vérification positive préalable de l'identité de l'usager ou de l'usagère;
d) la réinitialisation d'un mot de passe exige une vérification positive de l'identité de l'usager ou l'usagère avant que le mot de passe temporaire ne soit fourni;

e) lorsqu'un mot de passe est inclus dans un document par inadvertance (comme dans les demandes de service ou de mot de passe), le mot de passe du compte doit être changé immédiatement ou le compte doit être désactivé jusqu'à ce que le mot de passe puisse être changé;

f) la complexité des mots de passe doit être égale ou supérieure aux exigences prévues à cet égard.

De plus, les conditions d'emploi du personnel doivent prévoir l'obligation de maintenir la confidentialité des renseignements secrets d'authentification.

6.3.10 Mots de passe par défaut des fournisseurs

Les mots de passe par défaut des fournisseurs doivent être modifiés avant le déploiement du système ou du logiciel en question.

### 6.4 **Examen des droits d'accès des usagers**

Les droits d'accès accordés aux identificateurs d'utilisateur à l'égard de l'information et des systèmes d'information doivent être revus au moins à la fréquence indiquée ci-dessous :

a) Niveau non classifié :
   i. Ils sont revus une fois durant le cycle de vie ou lorsqu'un changement important est apporté au système d'information.
   ii. Ils sont revus par les propriétaires de l'information pour valider les contrôles d'accès nécessaires dans le cadre des exigences d'examen à l'égard du cycle de vie ou du changement important. Toute modification nécessaire découlant de cette revue doit être mise en œuvre par le Service des technologies de l'information ou le Service des installations et de la sécurité, selon le cas.

b) Niveau interne :
   i. Ils sont revus une fois durant le cycle de vie ou lorsqu'un changement important est apporté au système d'information.
   ii. Ils sont revus lorsqu'un changement dans l'emploi ou le rôle d'un usager ou d'une usagère touche son identificateur d'utilisateur.
   iii. Ils sont revus par les propriétaires de l'information pour valider les contrôles d'accès nécessaires dans le cadre des exigences d'examen à l'égard du cycle de vie ou du changement important. Toute modification nécessaire découlant de cette revue doit être mise en œuvre par le Service des technologies de l'information ou le Service des installations et de la sécurité, selon le cas.

c) Niveau confidentiel :
   i. Ils sont revus une fois durant le cycle de vie ou lorsqu'un changement important est apporté au système d'information.
   ii. Ils sont revus lorsqu'un changement dans l'emploi ou le rôle d'un usager ou d'une usagère touche son identificateur d'utilisateur.
   iii. Ils sont revus au moins une fois par an.
   iv. Ils sont revus par les propriétaires de l'information pour valider les contrôles d'accès nécessaires dans le cadre des exigences d'examen à l'égard du cycle de vie ou du changement important. Toute modification nécessaire découlant de cette revue doit être mise en œuvre par le Service des technologies de l'information ou le Service des installations et de la sécurité, selon le cas.

En outre, sans égard à la classification de sécurité, les vérifications qui suivent doivent être effectuées :

a) un rapport portant sur les identificateurs d'utilisateur ordinaires qui n'ont pas été utilisés depuis 90 jours (« comptes inactifs ») doit être généré au moins tous les trois mois en vue de l'examen par les gestionnaires appropriés, et tout compte non nécessaire doit être signalé et supprimé;

b) un rapport sur les identificateurs d'utilisateur dotés d'un accès privilégié qui n'ont pas été utilisés depuis 90 jours (« comptes privilégiés inactifs ») doit être généré au moins tous les trois mois en vue de l'examen par les gestionnaires appropriés, et tout compte privilégié inactif doit être désactivé immédiatement, sa réactivation nécessitant une nouvelle approbation.

## 6.5 **Contrôle de l'accès aux systèmes et aux applications**

### 6.5.1 Procédures d'ouverture de session sécuritaires

Lorsque le niveau de sécurité exige que l'ouverture d'une session soit effectuée par un identificateur d'utilisateur donné afin de contrôler l'accès, l'accès aux systèmes et aux applications doit être effectué au moyen d'une procédure d'ouverture de session sécuritaire répondant aux exigences minimales suivantes :

a) Niveau non classifié :
   i. Aucune exigence minimale.

b) Niveau interne :
   i. L'ouverture de session nécessite un identificateur d'utilisateur et un mot de passe.
   ii. Un registre des tentatives de connexion échouées doit être maintenu.

c) Niveau confidentiel :
   i. L'ouverture de session nécessite un identificateur d'utilisateur et le recours à une procédure d'ouverture de session à authentification à deux facteurs est fortement encouragé.
   ii. Les sessions doivent être désactivées après une période d'inactivité donnée.
   iii. Un registre des tentatives de connexion échouées doit être maintenu.

Lorsque la procédure d'ouverture de session est fondée sur l'utilisation d'un identificateur d'utilisateur et d'un mot de passe, la procédure doit protéger contre les activités qui suivent :

a) la divulgation d'information non nécessaire lors de l'échec de l'ouverture de session, en faisant en sorte que l'identificateur d'utilisateur et le mot de passe soient traités simultanément (sans qu'ils doivent nécessairement être saisis de cette façon) et que le système n'indique pas lequel de l'identificateur du mot de passe était fautif;
b) le vol de mot de passe en personne, en faisant en sorte que le mot de passe ne soit pas visible au moment de la saisie;
c) le vol d'authentifiants pendant le transit, en faisant en sorte qu'il soit obligatoire d'utiliser des méthodes de chiffrage approuvées par Service des technologies de l'information;
d) les tentatives d'attaque par force brute, en faisant en sorte qu'une fonction de délai croissant ou de verrouillage automatisé de l'identificateur d'utilisateur soit en place.

Les délais servant au verrouillage automatique pour inactivité et à la conservation des registres ainsi que le nombre maximal de tentatives échouées d'ouverture de session sont

fixés par le ou la responsable de l'information de concert avec le Service des technologies de l'information.

6.5.2 Système de gestion des mots de passe

Lorsque cela est possible, nous encourageons l'usage de phrases passe plutôt que de mots de passe plus simples.

Les systèmes de gestion des mots de passe doivent être interactifs et permettre à l'usagère ou l'usager de choisir son propre mot de passe, et devraient veiller à ce que des mots de passe de qualité soient utilisés au moyen des exigences suivantes :

a) les mots de passe courts ne sont pas permis;
b) l'usage de phrases passe plutôt que de mots de passe est encouragé en permettant l'emploi de longs mots de passe lorsque cela est techniquement possible;
c) les mots de passe sont vérifiés afin de prévenir l'usage de mots de passe déjà utilisés et, lorsque le système de gestion des mots de passe le permet, les mots de passe sont également vérifiés au moyen d'une liste de mots de passe à éviter, comme ceux qui correspondent à l'identificateur d'utilisateur, les mots courants tirés du dictionnaire, les séries séquentielles ou répétitives et les mots de passe capturés au cours de bris de sécurité antérieurs;
d) l'expiration des mots de passe devrait être gérée selon les normes actuelles établies par le Service des technologies de l'information;
e) les mots de passe sont conservés dans un format chiffré;
f) les indices permettant de se rappeler les mots de passe ne sont pas permis.

De plus, si l'authentification à deux facteurs est utilisée, le second facteur sera le plus rigide selon les capacités et les moyens disponibles.

Les exigences précises sur la complexité des mots de passe sont établies par le Service des technologies de l'information.

6.5.3 Usage de programmes de service privilégié

Les programmes de service qui pourraient avoir la capacité de contourner les contrôles des systèmes et des applications, comme les outils de craquage de mots de passe, ne sont pas permis au sein du périmètre de sécurité logique de l'Université et doivent être supprimés ou désactivés des installations par défaut.

Avec l'approbation des Services de technologie de l'information, une exception peut permettre un tel programme de service, mais les contrôles qui suivent sont obligatoires :

a) son utilisation est restreinte aux personnes nommément approuvées;
b) son utilisation n'est pas permise aux usagers et usagères qui ont accès à des systèmes où une séparation des tâches est nécessaire;
c) lorsqu'il n'est pas utilisé, le logiciel doit être supprimé des systèmes informatiques de l'Université et être conservé hors ligne séparément des autres logiciels d'application.

6.6 **Synchronisation des horloges**

Puisque les horloges internes de l'infrastructure informatique ont une incidence sur les systèmes d'authentification périodique et sur la capacité de comparer les données de connexion, ces horloges doivent se référer à la même source centrale d'authentification afin d'assurer leur synchronisation continue.

## 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_ Étiquetage et le traitement de l'information classifiée
7.7 Procédure_ Système de classification de l'information