UQAR Université du Québec à Rimouski

TITRE :	**DIRECTIVE RELATIVE À LA SÉCURITÉ DES IDENTIFIANTS ET DES MOTS DE PASSE**	**C3-D102**
RESPONSABILITÉ :	VICE-RECTORAT AUX RESSOURCES HUMAINES ET À L'ADMINISTRATION	
APPROUVÉ PAR :	COMITÉ EXÉCUTIF	RÉS. : EX-807-6074 (15-05-2018)
EN VIGUEUR :	15-05-2018	
MODIFIÉE :	EX-862-6665 (21-06-2022)	

Note : *Le texte que vous consultez est une codification administrative des documents normatifs de l'UQAR. La version officielle est contenue dans les résolutions adoptées par le Comité exécutif.*

TABLE DES MATIÈRES

1. ÉNONCÉ DE PRINCIPE ET OBJECTIFS

La directive précise les responsabilités et les règles à suivre en matière de gestion et de protection des identifiants et des mots de passe.

2. CADRE JURIDIQUE OU CADRE DE RÉFÉRENCE

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ c. G-1.03)
- *Directive relative à l'utilisation et à la gestion des technologies de l'information et des télécommunications* (C3-D30)
- *Politique de la sécurité de l'information* (C3-D99)
- *Cadre de gestion de la sécurité de l'information* (C3-D109)

3. CHAMP D'APPLICATION

La directive s'applique à la personne utilisatrice des systèmes, appartenant ou non à l'Université du Québec à Rimouski (Université), pour lesquels des informations en lien avec notre établissement sont collectées, utilisées, conservées, communiquées ou détruites.

4. DÉFINITION

4.1 « Personne utilisatrice » : désigne une personne faisant appel aux ressources informatiques de l'Université pour mener à bien ses activités.

4.2 « Identifiant » : information associée à une personne utilisatrice, connue de celle-ci ou contenue sur un support informatique dont elle est détentrice, et qui permet son identification. L'identifiant est unique et permet de reconnaitre la personne utilisatrice.

4.3 « Mot de passe » : information confidentielle détenue par une personne utilisatrice permettant de valider son identité lors de la procédure d'accès à un système informatique.

4.4 « Service/système externe » : désigne un service ou un système qui n'est pas supporté et/ou reconnu par le Service des technologies de l'information de l'Université. La liste des services/systèmes supportés et/ou reconnus est publiée sur le portail interne (Moodle) du Service des technologies de l'information.

4.5 « Authentification multifacteur » : est un procédé de vérification faisant appel à au moins deux (2) facteurs d'authentification différents.

5. SIGNALEMENT D'UN MANQUEMENT ET MESURES APPLICABLES

5.1 Toute personne qui est au fait d'un manquement à la présente directive doit le signaler à la coordonnatrice ou au coordonnateur de la sécurité de l'information [1].

5.2 Le non-respect de la directive peut entrainer la suspension des autorisations liées à un identifiant et peut entrainer des mesures disciplinaires.

6. AUTORISATIONS ET IDENTITÉ

6.1 L'identité d'une personne est validée par la combinaison d'informations suivantes : identifiant, mot de passe et, le cas échéant, un deuxième facteur d'authentification.

[1] Selon la *Politique de la sécurité de l'information,* le rôle de coordonnatrice ou de coordonnateur de la sécurité de l'information est confié à la direction du Service des technologies de l'information.

6.2 La personne utilisatrice est responsable des activités résultant de l'usage de son identifiant et des autorisations qui lui sont attribuées.

6.3 Les autorisations qui sont rattachées à un identifiant sont destinées à l'usage exclusif de la personne utilisatrice à qui elles sont attribuées.

6.4 La personne utilisatrice évitera d'utiliser des informations d'identification de l'Université (identifiant ou courriel) pour un service/système externe.

6.5 Nonobstant l'article 6.4, la personne utilisatrice qui doit utiliser des informations d'identification de l'Université pour un service/système externe doit choisir un mot de passe différent de celui utilisé à l'Université.

6.6 La personne utilisatrice ne doit pas usurper l'identité d'une autre personne.

6.7 La personne utilisatrice ne doit pas transmettre son mot de passe à une tierce personne ni permettre que son identifiant, son mot de passe et les autorisations qui y sont rattachées soient utilisés par une autre personne.

6.8 Nonobstant l'article 6.7, il est possible qu'une situation exceptionnelle ci-après décrite nécessite que la personne utilisatrice communique l'identifiant et mot de passe à une autre personne désignée. Le cas échéant, cette dernière utilisera l'identifiant pour un usage spécifique seulement. Lorsque l'usage spécifique est terminé, la personne utilisatrice doit modifier son mot de passe. Une situation exceptionnelle est présente lorsque les trois conditions suivantes sont réunies :

a) la continuité des activités de l'Université est compromise;

b) le système ne permet pas la délégation des privilèges;

c) le gestionnaire de l'information considère qu'il n'y a aucune autre option.

6.9 La personne utilisatrice qui croit que son identité est usurpée doit informer la coordonnatrice ou le coordonnateur de la sécurité de l'information de la situation et modifier son mot de passe le plus rapidement possible.

7. MOT DE PASSE

7.1 La personne utilisatrice doit prendre les mesures nécessaires afin de préserver la confidentialité de son mot de passe.

7.2 La personne utilisatrice qui croit que la confidentialité de son mot de passe est compromise doit modifier celui-ci dans les plus brefs délais. Elle doit aviser la coordonnatrice ou le coordonnateur de la sécurité de l'information de la situation.

7.3 La personne utilisatrice doit modifier un mot de passe lorsqu'elle en reçoit la demande explicite de la coordonnatrice ou du coordonnateur de la sécurité de l'information, de la personne détentrice de l'information ou de la personne supérieure immédiate.

7.4 Le Service des technologies de l'information détermine la fréquence de changement de mot de passe. La fréquence peut différer d'un système à l'autre. Lorsque la fréquence n'est pas déterminée, la personne utilisatrice doit modifier son mot de passe au moins une fois par année.

7.5 La personne utilisatrice doit respecter les critères de composition du mot de passe spécifique au système. Lorsque le système n'impose aucun critère de composition spécifique, la personne utilisatrice a la responsabilité, dans la mesure du possible, de choisir un mot de passe contenant au minimum douze (12) caractères et dont la composition respecte au minimum trois des règles suivantes :

- contenir au moins une lettre minuscule, contenir au moins une lettre majuscule**,** contenir au moins un chiffre

- contenir au moins un caractère spécial (@ # $ % ^ & * - _ ! + = [ ] { } | \ : ' ,. ? / ` ~ " ( ) ; < >)

7.6 La personne utilisatrice doit éviter de choisir un mot de passe facilement identifiable, à titre d'exemple : l'utilisation de son identifiant, numéro de téléphone, date de naissance, nom de son animal de compagnie, son adresse civique, etc.

7.7 La personne utilisatrice doit prendre soin de choisir un mot de passe différent de ceux utilisés antérieurement.

7.8 La personne utilisatrice ne doit pas utiliser un mot de passe unique pour tous ses identifiants.

7.9 Un mot de passe doit être chiffré lorsqu'il est entreposé sur un support informatique (fichier, base de données, stockage d'entreprise, etc.). La personne utilisatrice peut contacter le Centre de services TI (CSTI) pour plus d'information sur les moyens sécuritaires de stockage de mot de passe.

7.10 La personne utilisatrice doit mettre sous clé, en tout temps, les mots de passe conservés sur un support non informatique.

7.11 Un mot de passe ne doit pas être communiqué via des mécanismes non sécurisés : courriel, formulaire électronique non sécurisé/crypté.

7.12 La personne utilisatrice ayant un doute sur la légitimité d'une procédure d'accès ou d'authentification doit communiquer avec le Centre de Services TI (CSTI) pour assistance. Elle s'abstiendra de s'authentifier tant que le doute persiste.

8. RESPONSABILITÉS DES DIFFÉRENTES PERSONNES INTERVENANTES

Responsabilités en lien avec la Politique de la sécurité de l'information

8.1 La personne utilisatrice :

- prend connaissance et se conforme à la présente directive;
- signale tout manquement à la présente directive à la coordonnatrice ou au coordonnateur de la sécurité de l'information.

8.2 La coordonnatrice ou le coordonnateur de la sécurité de l'information (CSI) :

- maintient le registre des incidents en lien avec la sécurité des identifiants et des mots de passe;
- prend les actions appropriées à la suite d'un incident majeur touchant la sécurité des identifiants et des mots de passe;
- élabore, révise et coordonne la mise en œuvre de la présente directive.

8.3 La personne détentrice de l'information :

- s'assure que les membres de son unité administrative connaissent et appliquent la présente directive;
- informe la coordonnatrice ou le coordonnateur de la sécurité de l'information de tout manquement à la directive;
- collabore avec la coordonnatrice ou le coordonnateur de la sécurité de l'information afin d'identifier les problèmes liées à la sécurité des identifiants et des mots de passe.

8.4 Le Service des ressources humaines :

- assiste la personne supérieure immédiate de la personne utilisatrice dans la mise en place des mesures appropriées lors de la violation de la présente directive.

8.5 La personne responsable organisationnelle de la sécurité de l'information (ROSI) :

- appuie la coordonnatrice ou le coordonnateur de la sécurité de l'information ainsi que les principales personnes intervenantes, afin d'assurer la mise en place et le respect de la présente directive.

Responsabilités particulières à la présente directive

8.6 La personne supérieure immédiate de la personne utilisatrice :

- intervient à la demande de la coordonnatrice ou du coordonnateur de la sécurité de l'information, auprès des membres de son unité administrative afin de corriger les manquements à la présente directive;
- collabore avec la coordonnatrice ou le coordonnateur de la sécurité de l'information afin de sensibiliser les membres de son personnel sur la présente directive.