TITRE :	**POLITIQUE DE LA SÉCURITÉ DE L'INFORMATION**		
		CODE :	**C3-D99**
APPROUVÉ PAR :	CONSEIL D'ADMINISTRATION	RÉS. :	CA-654-8150 16-02-2016
EN VIGUEUR :	16-02-2016		
MODIFICATIONS :			

PRÉAMBULE

Les opérations de l'Université du Québec à Rimouski (UQAR) dépendent en grande partie de l'information qui est traitée, produite et communiquée. Cette information est très vaste et peut exister sur support papier ou technologique. Elle comprend, entre autres, les renseignements personnels des étudiantes et des étudiants, des membres du personnel, la propriété intellectuelle produite par le personnel enseignant et par les étudiantes et les étudiants, ainsi que la documentation interne stratégique et administrative.

Pour accomplir ses mandats, l'UQAR recueille, conserve, traite, diffuse et archive d'importantes quantités d'information dont la masse va toujours augmenter au fil des années. Ces informations sont nécessaires à la réalisation de sa mission et requièrent une protection tout au long de leur cycle de vie. Avec l'évolution des technologies de l'information, l'information numérique a pour sa part pris une place prépondérante dans les activités courantes de l'UQAR.

Comme toute autre institution d'enseignement supérieur, l'UQAR fait face à une multitude de menaces pouvant porter atteinte à la confidentialité, l'intégrité et la disponibilité de son information. Ces menaces, dont la nature est en constante évolution, comprennent, entre autres, le vol d'identité et d'information confidentielle, la fraude, l'espionnage industriel et le vol de propriété intellectuelle, l'utilisation, la divulgation et la destruction d'information, les défaillances techniques, les événements naturels et l'erreur humaine.

Par ailleurs, l'UQAR est soumise à plusieurs exigences légales, réglementaires ou contractuelles. Le respect de ces exigences et le lien de confiance qui existe envers l'UQAR de la part des membres du personnel, de la communauté étudiante et du public en général sont essentiels au maintien de sa réputation.

Il est donc impératif que l'UQAR protège adéquatement l'information qu'elle possède ou qui lui est confiée.

1. GÉNÉRALITÉS

OBJECTIF

Cette politique constitue un des éléments clés permettant d'assurer la réalisation de la mission et des objectifs stratégiques de l'UQAR, de maintenir sa réputation et de se conformer aux exigences légales, réglementaires et contractuelles applicables.

L'objectif principal de cette politique est de communiquer la détermination et l'engagement de l'UQAR de gérer avec efficacité et efficience les risques liés à la sécurité de l'information. L'approche préconisée vise l'identification des intervenantes et des intervenants, la définition de leurs rôles et la sensibilisation des usagères et des usagers aux différents risques. Cette politique vise également la conception et l'implantation de mesures qui assurent efficacement la sécurité des actifs informationnels.

PORTÉE

Cette politique s'applique à toutes les utilisatrices et les utilisateurs des ressources informationnelles de l'UQAR qui incluent, entre autres, les membres de la direction, les gestionnaires, les membres du personnel enseignant et le personnel de soutien, les étudiantes et les étudiants, de même que les personnes fournissant des biens ou des services, les personnes sous-traitantes et partenaires de l'UQAR.

Cette politique s'applique à toute l'information que détient l'UQAR dans le cours de ses activités ou dont elle a la garde, durant son cycle de vie, peu importe sa forme, son support et son emplacement.

Les principaux objectifs de la présente politique sont :

- se conformer aux lois, politiques et règlements applicables;
- assurer la disponibilité, l'intégrité et la confidentialité de l'information;
- assurer la confidentialité des renseignements personnels des étudiantes et des étudiants, des gestionnaires, des membres du personnel enseignant et du personnel de soutien de l'UQAR et de ses partenaires d'affaires;
- avoir une bonne connaissance des actifs informationnels à protéger ainsi que leur degré de sensibilité et en identifier les responsables.

2. RÔLES ET RESPONSABILITÉS

La présente politique et son application relèvent de différents intervenantes et intervenants à qui les mandats suivants sont attribués :

Conseil d'administration

- Approuve la politique ainsi que ses mises à jour.

Comité d'audit et des ressources humaines

- Recommande au Conseil d'administration l'adoption de la politique ainsi que ses mises à jour;
- veille à la mise en place de mécanismes assurant le respect de la politique;
- rend compte, au besoin, au Conseil d'administration.

La personne responsable de la sécurité de l'information/Direction du secrétariat général

- Valide la politique ainsi que ses mises à jour et recommande au comité d'audit et des ressources humaines son adoption par le Conseil d'administration;
- s'assure de l'application de la politique par les gestionnaires de l'information;
- s'assure que le programme de sécurité de l'information dispose des ressources financières et logistiques appropriées;
- dépose au dirigeant principal nommé par le Conseil du trésor un rapport sur l'état de la situation de la sécurité de l'information, selon les dates déterminées par le Conseil du trésor.

Mandats découlant de la fonction de la secrétaire générale ou du secrétaire général

- Interprète les lois et règlements pouvant avoir un impact sur la sécurité de l'information;
- communique les exigences légales, règlementaires et contractuelles applicables à la coordonnatrice ou au coordonnateur de la sécurité de l'information;
- valide les clauses contractuelles touchant à la sécurité de l'information, en collaboration avec la coordonnatrice ou le coordonnateur de la sécurité de l'information;

- s'assure que des mesures contractuelles adéquates sont prévues afin de protéger l'information et de se conformer à la présente politique;
- s'assure que la gestion des documents et des archives sont conformes à la présente politique et applique le cycle de vie de l'information conforme au Règlement 15 de l'UQAR;
- élabore et diffuse au besoin, en collaboration avec la coordonnatrice ou le coordonnateur à la sécurité de l'information et les autres intervenantes et intervenants, les politiques concernant la vie privée, la protection des renseignements personnels et la sécurité de l'information.

Coordonnatrice ou coordonnateur de la sécurité de l'information/direction du Service des technologies de l'information

- Élabore la politique et ses mises à jour et coordonne sa mise en œuvre;
- assiste les gestionnaires de l'information dans l'évaluation et la gestion des risques liés à la sécurité de l'information;
- identifie et maintient à jour la liste des actifs informationnels et de leur responsable;
- émet des directives, propose des solutions, coordonne leur mise en place et facilite la conformité en matière de sécurité de l'information;
- communique aux différents groupes de la communauté de l'UQAR leurs responsabilités respectives concernant la sécurité de l'information;
- élabore et met en œuvre le programme de sensibilisation à la sécurité de l'information pour les membres du personnel, en collaboration avec la direction du Service des ressources humaines;
- maintient le registre des incidents de sécurité de l'information et gère le processus hiérarchique et de résolution de problème dans ce domaine;
- effectue le suivi des observations et des recommandations des utilisatrices et des utilisateurs en matière de sécurité de l'information;
- intervient en tout temps pour confirmer l'existence ou le bon fonctionnement d'une mesure de sécurité ou pour émettre des recommandations, si les actifs informationnels de l'UQAR sont jugés à risque;
- communique les risques à la sécurité de l'information et rend compte de l'application de la présente politique à la personne responsable de la sécurité de l'information;
- prend les actions appropriées à la suite d'un incident majeur touchant à la sécurité de l'information, en collaboration avec la direction du Service des ressources humaines;
- développe et met en œuvre les directives, processus, standards et procédures touchant à la sécurité des actifs informationnels, dont notamment la gestion des accès, la gestion des incidents et l'intégrité de l'information;
- développe, intègre et maintient des mesures de sécurité correspondant au niveau de sensibilité de l'information et autres exigences d'affaires, légales, règlementaires ou contractuelles applicables.

Gestionnaires de l'information

- Agit en tant que la personne responsable désignée par son unité administrative en appliquant les dispositions de la présente politique;
- établit et révise périodiquement les profils d'accès des utilisatrices et des utilisateurs et les communique aux intervenantes et intervenants concernés;
- s'assure du respect des exigences légales, règlementaires et contractuelles applicables à la sécurité de l'information pour son secteur, en collaboration avec la coordonnatrice ou le coordonnateur à la sécurité de l'information;
- évalue les risques à la sécurité de l'information pour son secteur en collaboration avec la coordonnatrice ou le coordonnateur de la sécurité de l'information;
- accepte, au nom de son unité administrative, les risques résiduels à la sécurité de l'information.

Direction du* S*ervice des ressources humaines

- Vérifie, au besoin, les antécédents des candidates et des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information;
- appuie la coordonnatrice ou le coordonnateur de la sécurité de l'information lors de l'élaboration et de la mise en œuvre du programme de sensibilisation à la sécurité de l'information pour les membres du personnel;
- intervient auprès des membres du personnel concernés en cas d'atteinte à la sécurité de l'information, en collaboration avec la coordonnatrice ou le coordonnateur de la sécurité de l'information ainsi que les autres intervenantes ou intervenants;
- prend des mesures, fait le suivi et impose les sanctions appropriées lors de violation des politiques, règlements et directives touchant à la sécurité de l'information, en collaboration avec la supérieure ou le supérieur immédiat;
- informe les gestionnaires de l'information concernés d'une embauche, d'un changement de fonctions, d'une mutation et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels.

Utilisatrices ou utilisateurs

- Prend connaissance et adhère aux politiques, règlements et autres directives pertinentes de l'UQAR touchant à la sécurité de l'information qui le concernent;
- utilise les actifs informationnels, en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont accordés;
- rapporte à son gestionnaire de l'information tout incident qui met ou a pu mettre en péril la sécurité de l'information.

CADRE LÉGAL ET ADMINISTRATIF

La politique s'inscrit, entre autres, dans le contexte législatif de :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03, a. 20);
- *Charte des droits et libertés de la personne du Québec* (RLRQ, c. C-12, a. 5 et a. 44);
- *Code civil du Québec* (RLRQ, c. C-1991, a. 37 à 41);
- *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1);
- *Loi sur les archives* (RLRQ, c. A-21.1);
- *Loi sur le droit d'auteur* (L.R.C (1985) ch. C-42);
- *Code criminel* (L.R.C. (1985) ch. C-46);
- Règlement 15 : *Registres officiels et documentation administrative de l'Université du Québec à Rimouski*.

ANNEXE A : PLAN DE COMMUNICATION DE LA POLITIQUE DE LA SÉCURITÉ DE L'INFORMATION