UQAR Université du Québec à Rimouski

TITRE : **CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION** **C3-D109**

RESPONSABILITÉS : VICE-RECTORAT AUX RESSOURCES HUMAINES ET À L'ADMINISTRATION
SECRÉTARIAT GÉNÉRAL ET VICE-RECTORAT À LA VIE ÉTUDIANTE

APPROUVÉE : CONSEIL D'ADMINISTRATION RÉSOLUTION : CA-757-9211
21-06-2022

EN VIGUEUR : 21-06-2022

MODIFICATION :

***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 Conseil d'administration.*

## TABLE DES MATIÈRES

# 1. INTRODUCTION

## 1.1 Contexte

Le présent cadre de gestion est adopté en application de l'article 12 de la Directive sur la sécurité de l'information gouvernementale. Celle-ci fait obligation aux organismes publics d'adopter et de mettre en œuvre un cadre de gestion de la sécurité de l'information, de le maintenir à jour et d'en assurer l'application.

## 1.2 Définitions

**Actif informationnel** : Systèmes d'information, réseau de télécommunication, infrastructure technologique ou un ensemble de ces éléments contenant un document. Est également considéré comme un actif informationnel l'information regroupée dans un système d'information ou un support papier contenant un document.

**Document** : Ensemble constitué d'informations portées par un support. L'information y est délimitée et structurée de façon tangible ou logique, selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles. Est aussi considérée comme document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

**Événement de sécurité** : Toute forme d'atteinte, présente ou appréhendée, comme une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'un actif informationnel sous la responsabilité d'un organisme public ou d'une personne agissant pour ce dernier.

**Personne détentrice de l'information** : Personne employée désignée par la personne responsable organisationnelle de la sécurité de l'information (ROSI), appartenant à la classe d'emploi de niveau cadre, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité de son unité administrative.

**Pilote de système d'information** : Personne nommée par la personne détentrice de l'information afin de configurer un système d'information en fonction des besoins des personnes utilisatrices. Elle est responsable d'encadrer et de valider l'utilisation adéquate du système afin d'assurer un accès à l'information dans le respect du cadre normatif de la sécurité de l'information.

**Personne utilisatrice** : Toute personne de l'Université du Québec à Rimouski (l'Université) de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'Université ou y a accès.

**Système d'information :** Ensemble organisé de ressources matérielles et logiciels permettant d'acquérir, de conserver, de traiter et de diffuser les éléments d'informations.

**Registre des événements de sécurité :** Le registre regroupe les informations relatives aux événements de sécurité, notamment les coordonnées du chef de la sécurité de l'information organisationnelle (courriel, téléphone), la date, l'heure, la localisation (adresse), la nature ainsi que la description de l'événement. Il contient aussi les préjudices engendrés et les personnes morales ou physiques concernées, les actions prises, l'acceptation ou non du risque résiduel et les justificatifs afférents, les actions prévues et la date de clôture de l'événement.

### 1.3 Cadre légal et administratif

Le cadre de gestion s'inscrit principalement dans un contexte régi par :

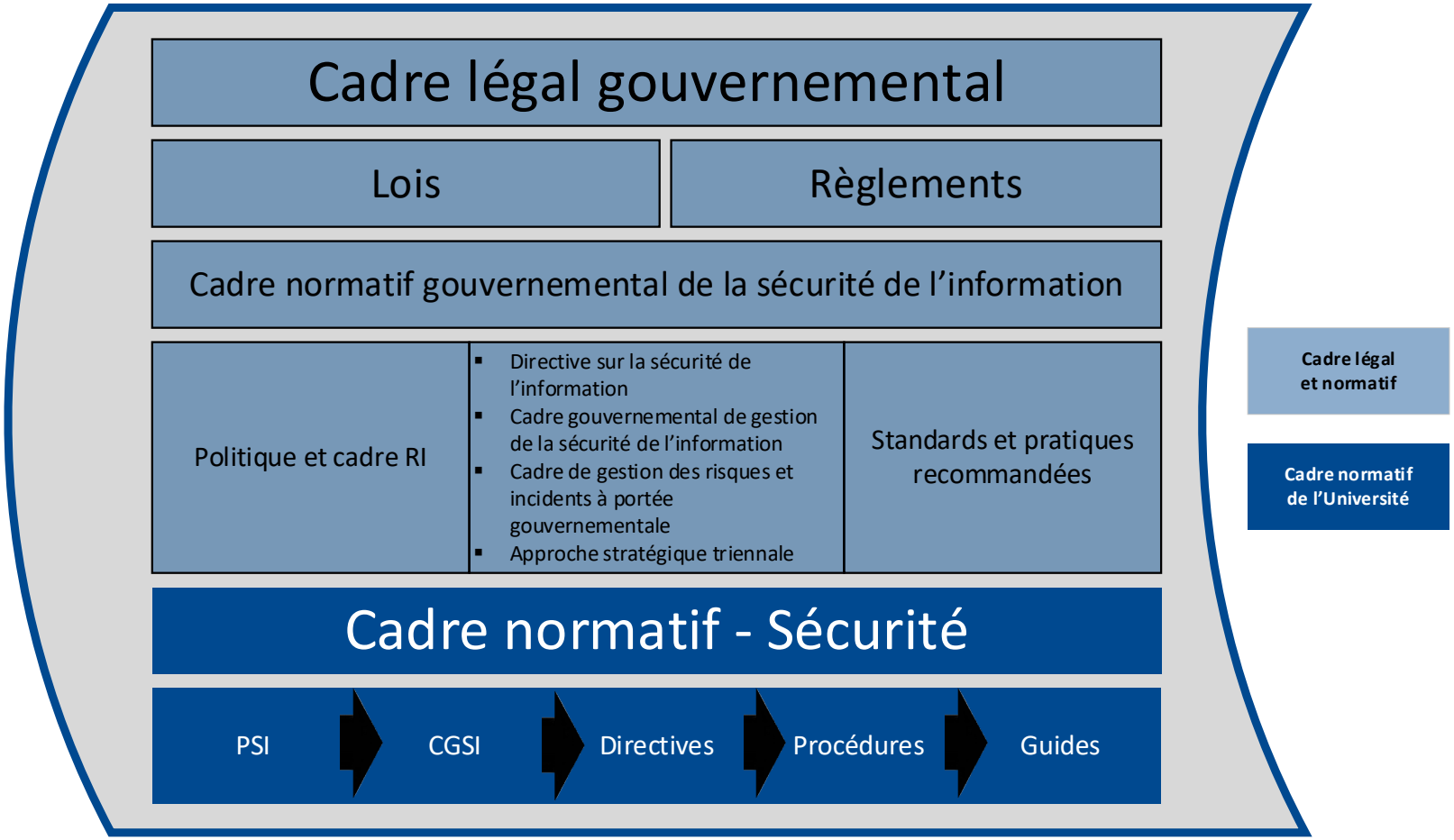
- la *Loi sur l'Université du Québec* (RLRQ, ch. U-1);
- la *Charte des droits et libertés de la personne* (RLRQ, ch. C-12);
- le *Code civil du Québec* (RLRQ,, ch. CCQ-1991);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, ch. G-1.03);
- la *Loi concernant le cadre juridique des technologies et l'information* (RLRQ, chapitre C- 1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- la *Loi sur les archives* (RLRQ, chapitre A-21.1);
- la *Loi canadienne sur les droits de la personne* (LRC, 1985, chapitre H-6);
- le *Code criminel* (LRC, 1985, chapitre C-46);
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r. 02);
- la *Directive sur la sécurité de l'information gouvernementale*;
- le *Règlement 15 : Registres officiels et documentation administrative de l'UQAR*.

### 1.4 Objectif

Le présent cadre de gestion a pour objectif de compléter les dispositions de la *Politique de sécurité de l'information* de l'Université et de renforcer la gouvernance de la sécurité de l'information au sein de celle-ci, par la mise en place d'une structure fonctionnelle de la sécurité de l'information et par la définition des rôles et responsabilités des personnes intervenant en la matière.

Ce cadre s'appuie sur les cadres légal et normatif du gouvernement ainsi que sur la Politique de sécurité de l'information de l'Université tel qu'illustré ci-dessous.

**Figure 1 : Positionnement du cadre de gestion de la sécurité de l'information de l'Université**



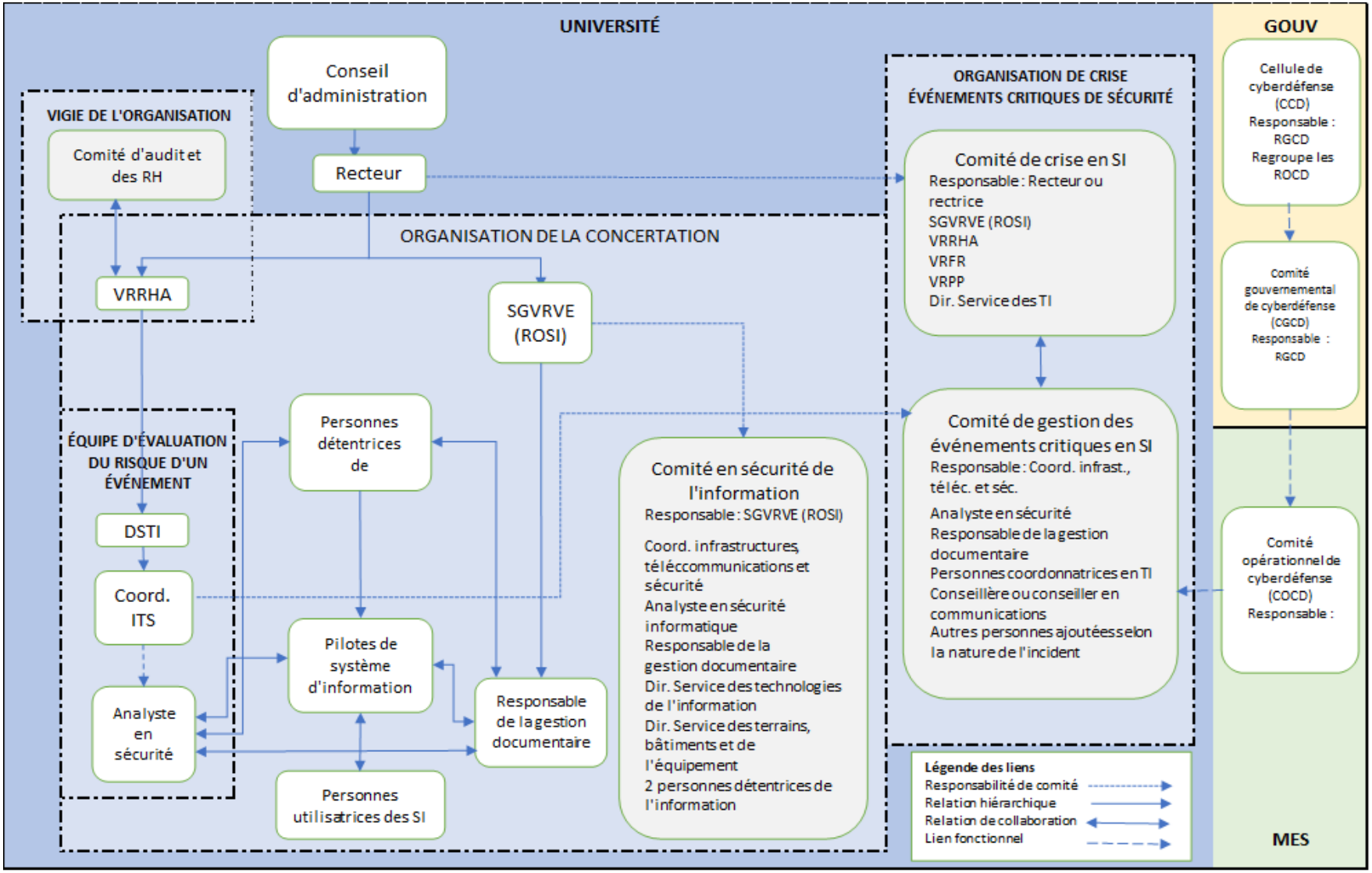

PSI : Politique de Sécurité de l'Information
CGSI : Cadre de Gestion de la Sécurité de l'Information

## 2. ORGANISATION FONCTIONNELLE EN SÉCURITÉ DE L'INFORMATION

La structure fonctionnelle mise en place à l'Université vise à organiser efficacement les activités s'appliquant à déterminer, évaluer et gérer les risques d'atteinte à la sécurité de l'information. Elle répartit les rôles et responsabilités à des personnes occupant des fonctions au sein de l'Université de manière à favoriser une prise en charge complète de la sécurité de l'information. Un minimum de comités est ajouté afin de favoriser la collaboration et la cohésion efficiente entre les diverses personnes intervenantes.

Le lien formel avec la structure de sécurité du ministère de l'Enseignement supérieur (MES) est assuré par la personne responsable organisationnelle de la sécurité de l'information (ROSI).

**Figure 2 : Illustration de l'organisation fonctionnelle pour assurer la sécurité de l'information**



## 3. RÔLES ET RESPONSABILITÉS DES PERSONNES INTERVENANTES

Les rôles et responsabilités des personnes intervenantes clés en matière de sécurité de l'information sont attribués comme suit :

### 3.1 La rectrice ou le recteur

À titre de personne dirigeante principale de l'information pour l'Université, elle est la première responsable en matière de sécurité de l'information. À ce titre, cette personne :

- veille au respect des orientations stratégiques de la sécurité de l'information gouvernementale;
- s'assure de la mise en œuvre des processus officiels de sécurité de l'information permettant, notamment, de veiller à la gestion des risques, à la gestion de l'accès à l'information et à la gestion des événements;
- désigne la personne responsable organisationnelle de la sécurité de l'information (ROSI).

### 3.2 La personne responsable organisationnelle de la sécurité de l'information (ROSI)

La secrétaire générale et vice-rectrice ou le secrétaire général et vice-recteur à la vie étudiante assume le rôle de personne responsable organisationnelle de la sécurité de l'information. Elle joue le rôle de porte-parole de la rectrice ou du recteur en matière de sécurité de l'information et lui fait part de ses réalisations. À cet égard, cette personne :

- assure la coordination et la cohérence des actions de sécurité de l'information menées au sein de l'Université par d'autres personnes intervenantes notamment, les personnes détentrices de l'information ainsi que les personnes responsables des actifs informationnels, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;
- désigne les personnes détentrices de l'information et leur attribue les responsabilités définies par le présent cadre de gestion;
- approuve les bilans de sécurité de l'information;
- s'assure que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comprennent des clauses garantissant le respect des exigences de sécurité de l'information;
- s'assure de l'existence d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
- participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information liées à son champ de responsabilité.

### 3.3 La directrice ou le directeur du Service des technologies de l'information (DSTI)

La directrice ou le directeur du Service des technologies de l'information apporte au niveau tactique son soutien à la personne ROSI, notamment en ce qui concerne la mise en œuvre des mesures de sécurité et la mise en place des processus officiels de sécurité de l'information. À cet égard, cette personne :

- soumet, aux fins de consultation, au comité chargé de la sécurité de l'information, les orientations, les politiques, les directives, les cadres de gestion, les priorités d'actions, les éléments de reddition

de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;

- s'assure de la réalisation périodique d'audits de sécurité de l'information et de tests d'intrusion et de vulnérabilités conformément aux énoncés de la Directive sur la sécurité de l'information gouvernementale et en dégage les priorités d'actions ainsi que les échéanciers afférents;
- met en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;
- produit les bilans et les plans d'action de sécurité de l'information et les soumet aux instances gouvernementales après approbation;
- favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor;
- s'assure de l'élaboration et de la mise en œuvre d'un programme de formation et de sensibilisation en matière de sécurité de l'information;
- s'assure de la contribution de l'Université au processus de gestion des risques et des événements de sécurité de l'information à portée gouvernementale;
- déclare au dirigeant principal de l'information du MES les risques de sécurité de l'information à portée gouvernementale;
- déclare à l'organisme désigné par le gouvernement les événements de sécurité de l'information et les risques à portée gouvernementale;
- définit et met en œuvre les processus officiels de sécurité de l'information dont notamment la gestion des risques, la gestion de l'accès à l'information et la gestion des événements;
- s'assure de l'élaboration et de la mise en œuvre des directives, des guides et des procédures en lien avec la sécurité de l'information;
- s'assure de la conception, de la réalisation et de la documentation des fonctionnalités de sécurité des systèmes d'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels et de leur intégration aux systèmes d'information en s'assurant de leur bon fonctionnement;
- participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information liées à son champ de responsabilité.

### 3.4 La coordonnatrice ou le coordonnateur des infrastructures, des télécommunications et de la sécurité (CITS)

La coordonnatrice ou le coordonnateur des infrastructures, des télécommunications et de la sécurité apporte, au niveau opérationnel, son soutien au DSTI et à la personne ROSI, notamment en ce qui concerne la coordination et la mise en œuvre des directives et des processus officiels en matière de sécurité de l'information et de gestion des événements. À cet égard, la personne :

- coordonne et participe au processus de catégorisation de l'information et d'analyses de risques de sécurité de l'information avec les personnes détentrices d'information;
- coordonne et participe à l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;
- s'assure de la mise à jour du registre d'autorité de la sécurité de l'information;
- s'assure de la mise à jour de l'inventaire des actifs informationnels servant au support numérique de l'information;

- propose au DSTI des orientations, des plans d'action et des bilans;
- assure la coordination et la réalisation de projets de sécurité de l'information;
- coordonne la mise en place du processus de gestion des événements de sécurité de l'information et du processus gouvernemental de gestion des événements;
- coordonne la tenue du registre des événements ayant pu mettre en péril la sécurité de l'information, documente ces événements et en tient informés le DSTI et la personne ROSI;
- coordonne et participe à l'analyse des risques de sécurité de l'information, à la détermination des menaces et des situations de vulnérabilité et assure la mise en œuvre des solutions appropriées;
- assure la coordination de l'équipe de réponse aux événements de sécurité de l'information et met en œuvre les stratégies de réaction appropriées;
- coordonne et collabore aux tests de relève planifiés qui ont lieu afin d'assurer le maintien des services en situation d'événement;
- élabore et met en œuvre des directives, des guides et des procédures reliés à la sécurité de l'information;
- participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information liées à ses champs de responsabilité.

### 3.5 L'analyste en sécurité

L'analyste en sécurité apporte son soutien au CITS et au DSTI en ce qui concerne l'opérationnalisation des directives et des processus officiels en matière de sécurité de l'information et de gestion des événements. À cet égard, la personne :

- assiste les personnes détentrices dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information;
- participe à l'élaboration et à la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;
- maintient à jour le registre d'autorité de la sécurité de l'information;
- maintient à jour l'inventaire des actifs informationnels servant au support numérique de l'information (les systèmes d'information, le réseau de télécommunication et les infrastructures technologiques);
- participe à la rédaction et à la préparation des plans d'action et des bilans;
- participe à la réalisation de projets de sécurité de l'information;
- contribue à la mise en place du processus de gestion des événements de sécurité de l'information et du processus gouvernemental de gestion des événements;
- maintient à jour le registre des événements de sécurité de l'information, documente ces événements et en tient informés le CITS et le DSTI;
- analyse les risques de sécurité de l'information, détermine les menaces et les situations de vulnérabilité et recommande la mise en œuvre de solutions de remédiation appropriées;
- participe aux activités de réponse aux événements de sécurité de l'information en appliquant les stratégies de réaction appropriées;
- contribue aux tests de relève planifiés qui ont lieu afin d'assurer le maintien des services en situation d'événement;

- participe à la rédaction des directives, des procédures et des guides propres à son domaine d'intervention;
- participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information liées à ses champs de responsabilité.

### 3.6 Les personnes détentrices de l'information

Les personnes détentrices de l'information désignées par la personne ROSI sont responsables ultimes de l'information qu'elles détiennent. À cet égard, elles :

- maintiennent les informations relatives aux actifs informationnels sous leur responsabilité;
- catégorisent l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité;
- agissent comme maîtres d'œuvre des analyses de risques et s'assurent de la prise en charge des risques résiduels;
- participent, au besoin, à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans;
- collaborent, avec la personne responsable de l'accès aux documents et de la protection des renseignements personnels, à la mise en place et à l'application des mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels;
- s'assurent de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;
- s'assurent de la mise en place d'un plan de continuité des activités;
- collaborent aux tests de relève planifiés qui ont lieu afin d'assurer le maintien des services en situation d'événement.

### 3.7 La ou le pilote de système d'information

Cette personne est désignée par la personne détentrice de l'information. Elle est chargée de mettre en application le cadre de gestion de la sécurité de l'information. À cet égard, cette personne :

- vérifie le respect des règles de sécurité du système d'information par les personnes utilisatrices et informe la personne détentrice en cas de manquement;
- applique et contrôle les règles logiques d'accès à un système d'information et gère les accès (création-modification-désactivation);
- informe les personnes utilisatrices de leurs obligations face à l'utilisation d'un système d'information;
- rend des comptes à la personne détentrice de l'information du fonctionnement général du système d'information (rendement, événements/accidents, développement, etc.);
- élabore le plan de relève du système d'information, le fait approuver par la personne détentrice, le diffuse et assure sa mise à jour;
- participe à la planification et à la coordination de la formation et, lorsque requis, forme les personnes utilisatrices;
- assiste et supporte les personnes utilisatrices;

- évalue régulièrement les processus afin d'optimiser ceux-ci;
- participe à la détermination des besoins;
- effectue des tests de bon fonctionnement du système et participe, au besoin, à ceux des équipements;
- participe aux tests de relève planifiés qui ont lieu afin d'assurer le maintien des services en situation d'événement.

### 3.8 Les personnes cadres

En plus de leurs responsabilités de personnes détentrices d'actif informationnel, les personnes cadres sont responsables de la mise en œuvre des dispositions de la Politique de sécurité de l'information auprès du personnel relevant de leur autorité. Principalement, ces personnes :

- informent leur personnel des dispositions de la Politique sur la sécurité de l'information et de toute directive, procédure et guide en vigueur en matière de sécurité de l'information ainsi que des modalités liées à leur mise en œuvre et le sensibilisent à la nécessité de s'y conformer;
- s'assurent que les actifs informationnels mis à la disposition de leur personnel sont utilisés en conformité avec les principes généraux et les exigences de la Politique sur la sécurité de l'information;
- s'assurent que la sécurité de l'information est prise en compte dans tout contrat de service attribué par leur unité administrative et voient à ce que tout consultante, consultant, partenaire ou fournisseur s'engagent à respecter et respectent les règles de sécurité de l'information de l'Université.

### 3.9 La personne responsable de l'architecture de sécurité de l'information

Cette responsabilité est assumée par la personne coordonnatrice des infrastructures, des télécommunications et de la sécurité (CITS). Notamment, elle :

- conçoit et met en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;
- arrime les solutions retenues aux processus organisationnels de sécurité de l'information;
- participe à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires, élaborées ou acquises par l'Université.

### 3.10 La personne responsable de la gestion des technologies de l'information (RGTI)

Cette responsabilité est assumée par la directrice ou le directeur du Service des technologies de l'information (DSTI). Notamment, cette personne :

- met en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par son organisation, dont les plans de reprise informatique en cas de sinistre;
- s'assure de la mise en place d'un cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

### 3.11 La personne responsable de l'accès à l'information et de la protection des renseignements personnels

Cette responsabilité est assumée par la secrétaire générale et vice-rectrice ou le secrétaire général et vice-recteur à la vie étudiante. Cette personne veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1). À ce titre, elle :

- contribue à assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des événements de sécurité de l'information.

### 3.12 La personne responsable de la gestion documentaire

Cette responsabilité est assumée par l'archiviste de l'Université. Cette personne :

- collabore à la conception des systèmes informatiques, administratifs ou autres et s'assure qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois;
- collabore étroitement avec les personnes détentrices de l'information et les autres personnes intervenantes en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité, indépendamment de son support;
- maintient à jour l'inventaire des documents incluant leur évaluation en termes de disponibilité, d'intégrité et de confidentialité.

### 3.13 La personne responsable de la sécurité physique

La directrice ou le directeur du Service des terrains, bâtiments et de l'équipement est responsable de la sécurité physique et met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle. Notamment, cette personne :

- conçoit et met en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, les accès non contrôlés, le vol ainsi que l'interruption des activités de l'Université;
- s'assure de la mise au rebut sécuritaire des supports de l'information;
- élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

### 3.14 La vice-rectrice ou le vice-recteur aux ressources humaines et à l'administration

La vice-rectrice ou le vice-recteur à l'administration et aux ressources humaines exerce une vigie en matière de sécurité de l'information, plus particulièrement en ce qui a trait à la détermination, à l'évaluation et à la gestion des risques d'atteinte à la sécurité de l'information. Elle ou il fait état de ses constatations au Comité d'audit et des ressources humaines et à la personne ROSI. Dans le cadre de sa vigie, cette personne :

- évalue l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre;
- examine l'adéquation de l'intégration de la sécurité de l'information dans les processus de l'Université;
- vérifie l'intégration de l'éthique dans les processus de gestion de la sécurité de l'information afin d'assurer la régulation des conduites et la responsabilisation individuelle.

## 4. RÔLES ET RESPONSABILITÉS DES INSTANCES ET DES COMITÉS

Les rôles et responsabilités des comités en matière de sécurité de l'information sont attribués comme suit :

### 4.1 Le conseil d'administration

Il adopte la Politique de sécurité de l'information et le Cadre de gestion de la sécurité de l'information.

### 4.2 Le comité exécutif

Il adopte les directives découlant de la Politique de sécurité de l'information et du cadre de gestion de la sécurité de l'information.

### 4.3 Le comité d'audit et des ressources humaines

Il assure une vigie des activités en matière de sécurité de l'information par l'entremise des constatations soumises par la vice-rectrice ou le vice-recteur aux ressources humaines et à l'administration.

### 4.4 Le comité en sécurité de l'information

Présidé par la personne responsable organisationnelle de la sécurité de l'information (ROSI) ce comité a pour mandat d'appuyer cette dernière quant aux mesures à mettre en place pour assurer le respect de la Politique de sécurité de l'information et du présent cadre de gestion. Il est la principale instance de concertation en matière de sécurité de l'information. Plus particulièrement, il :

- examine et formule des recommandations concernant les orientations, les politiques, les directives, le cadre de gestion, les plans d'action et les bilans de l'Université ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information;
- analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'Université.

Il est composé de la personne CITS, de l'analyste en sécurité informatique, de la personne responsable de la gestion documentaire, de la directrice ou du directeur du Service des technologies et de l'information, de la directrice ou du directeur du Service des terrains, bâtiments et de l'équipement, de deux (2) personnes représentant les personnes détentrices de l'information et de deux (2) personnes représentant les pilotes de systèmes d'information.

Le comité peut s'adjoindre toute autre personne pouvant contribuer aux échanges selon les sujets abordés. Deux (2) rencontres sont prévues annuellement.

### 4.5 Comité de gestion des événements critiques

Le comité de gestion des événements critiques est sous la responsabilité de la personne coordonnatrice des infrastructures, des télécommunications et de la sécurité (CITS) en TI. Il a pour rôle, notamment :

- de s'assurer de la réalisation des actions pour contrer la menace, atténuer les impacts, corriger les vulnérabilités;
- de suivre l'évolution d'un événement et d'en informer le comité de gestion de crise;
- d'appliquer le plan de gestion des événements;
- de procéder à l'évaluation des dommages;
- d'assurer le retour à la normale;
- de recommander au comité de gestion de crise la production d'une déclaration de sinistre;
- d'assurer la coordination avec les intervenantes et les intervenants externes.

Le comité est composé de l'analyste en sécurité, des personnes coordonnatrices au Service des technologies de l'information, de la personne responsable de la gestion documentaire et d'une conseillère ou d'un conseiller en communications.

Il peut s'adjoindre toute autre personne en mesure de contribuer à ses travaux selon la nature de l'événement.

### 4.6 Le comité de gestion de crise

Ce comité est sous la responsabilité du recteur ou de la rectrice. En cas d'événement critique de sécurité de l'information, il doit supporter le comité de gestion des événements et tenir compte de ses recommandations.

Ce comité est appelé à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des activités. À ce titre, il doit assurer :

- la mise en œuvre de stratégies permettant d'assurer la prise en charge des événements critiques de sécurité de l'information;
- la déclaration de sinistre à l'assureur;
- l'approbation des budgets spéciaux pour la gestion de l'événement;
- la décision du déploiement ou non des plans de continuité des activités;
- l'orientation à suivre et des actions à prendre en cas de sinistre;
- le délestage, en totalité ou en partie, des activités de l'Université;
- les communications.

Il est composé de la secrétaire générale et vice-rectrice ou du secrétaire général et vice-recteur à la vie étudiante, de la vice-rectrice ou du vice-recteur aux ressources humaines et à l'administration, de la vice-rectrice ou du vice-recteur à la formation et à la recherche, de la vice-rectrice ou du vice-recteur à la planification et aux partenariats, de la directrice ou du directeur du Service des technologies de l'information et de la directrice ou du directeur du Service des communications.

Le comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décisions.

## 5. DISPOSITIONS FINALES

Le présent cadre de gestion de la sécurité de l'information est complémentaire à la *Politique de sécurité de l'information de l'Université*. Il entre en vigueur à la date de son approbation par le Conseil d'administration et demeure en application tant et aussi longtemps qu'il n'est pas abrogé, modifié ou remplacé par un autre cadre de gestion.