Cadre de gestion de la sécurité de l'information

ADOPTION		
Instance	**Date**	**Décision**
Conseil d'administration	2017-12-05	CAD-11520

MODIFICATION			
Instance	**Date**	**Décision**	**Commentaires**
CAD			

RÉVISION	Aux trois (3) ans
Responsable	Vice-recteur aux affaires administratives
Partie prenante	Service des technologies de l'information (responsable de la sécurité de l'information)
CODE DE CLASSIFICATION	1164-05.003-1

Table des matières

1. Dispositions générales

1.1 Préambule

Le présent cadre vient en complément de la *Politique relative à la sécurité des actifs informationnels.* Ce cadre de gestion est adopté en application du paragraphe (a) du premier alinéa de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale*. La *Directive* oblige les organismes publics à adopter, à maintenir, à mettre à jour et à mettre en œuvre une politique et un cadre de gestion en matière de sécurité de l'information, qui viennent se joindre au cadre gouvernemental de gestion de la sécurité. Ayant comme base le document guide du Conseil du trésor, mais adapté à la réalité organisationnelle, il permettra de prendre en compte les exigences gouvernementales.

1.2 Objectifs

- Renforcer la gouvernance de la sécurité de l'information de l'Université du Québec à Chicoutimi, par la mise en place d'une structure organisationnelle de la sécurité de l'information et la définition des rôles et responsabilités de façon plus spécifique.
- Établir une gouvernance forte et intégrée de la sécurité de l'information à l'intérieur de l'Université du Québec à Chicoutimi.

1.3 Champ d'application

Le champ d'application du présent cadre de gestion est le même que celui de la *Politique relative à la sécurité des actifs informationnels*.

1.4 Définitions

Aux fins d'application du présent cadre de gestion, les expressions suivantes se définissent comme suit :

« Actif informationnel » : Tel que défini dans la *Politique relative à la sécurité des actifs informationnels*.

« Détenteur d'information » : Un employé désigné par l'UQAC, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, 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. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

« Ressources informationnelles » : Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

« Utilisateur d'actifs informationnels » : Toute personne de l'UQAC de toute catégorie d'emploi, de statut d'employé, d'étudiant ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'UQAC ou y a accès.

2. La structure fonctionnelle du gouvernement

Sur le plan organisationnel, les rôles et responsabilités sont assignés à chaque dirigeant d'organisme public, au dirigeant réseau de l'information (DRI), au dirigeant sectoriel de l'information (DSI), au responsable organisationnel de la sécurité de l'information (ROSI), au conseiller organisationnel en sécurité de l'information (COSI), au coordonnateur organisationnel de gestion des incidents (COGI), aux responsables des domaines connexes à la sécurité de l'information et aux comités sectoriels en sécurité de l'information.

Ainsi, le dirigeant d'organisme public est le premier responsable de la sécurité de l'information relevant de son autorité. À ce titre, il doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques de sécurité de l'information.

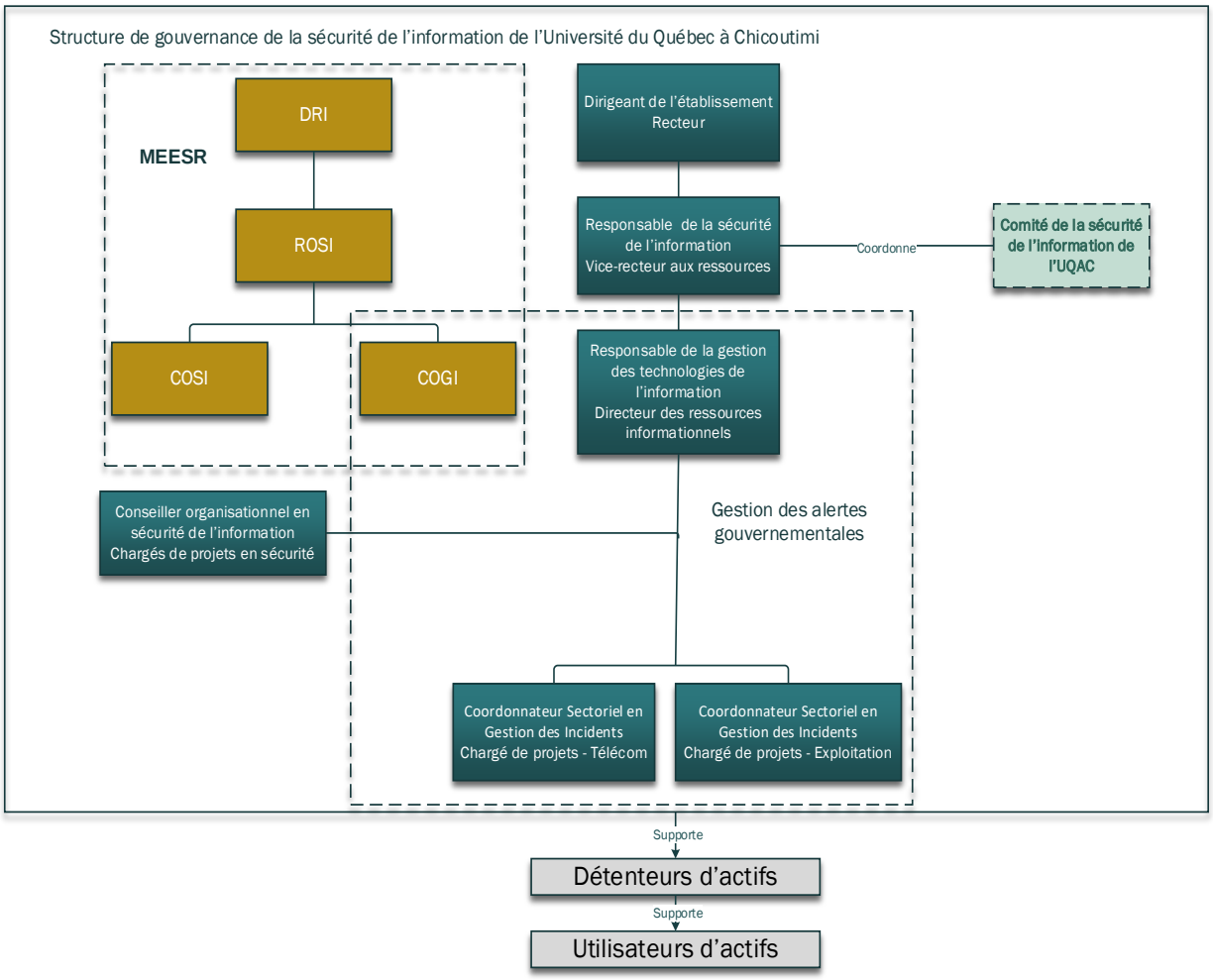
Le DRI et le DSI, respectivement désignés en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03)*, veillent à l'application, par les organismes publics qui leur sont rattachés, des règles de gouvernance et de gestion établies en matière de sécurité de l'information.

Le ROSI, quant à lui, joue le rôle de porte-parole du DPI auprès de son organisation, à laquelle il communique les orientations et les priorités d'intervention gouvernementales en sécurité de l'information. Il assure également la coordination et la cohérence des actions en matière de sécurité de l'information qui sont posées par d'autres intervenants au sein de son organisation. De plus, il coordonne la contribution de son organisation aux processus de gestion des risques et de gestion des incidents à portée gouvernementale.

Le COSI apporte son soutien au ROSI au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information.

Le COGI collabore étroitement avec le ROSI et le COSI, en leur fournissant le soutien technique nécessaire à l'exercice de leurs responsabilités. Il participe activement au réseau d'alerte gouvernemental et contribue à la mise en place du processus de gestion des incidents au sein de son organisation et du processus de gestion des incidents à portée gouvernementale.

Par ailleurs, le présent cadre de gestion précise les rôles des intervenants en matière de sécurité des actifs informationnels à l'UQAC.


Structure de gouvernance de la sécurité de l'information de l'Université du Québec à Chicoutimi
MEESR
DRI
ROSI
COSI
COGI
Dirigeant de l'établissement
Recteur
Responsable de la sécurité de l'information
Vice-recteur aux ressources
Coordonne
Comité de la sécurité de l'information de l'UQAC
Responsable de la gestion des technologies de l'information
Directeur des ressources informationnels
Conseiller organisationnel en sécurité de l'information
Chargés de projets en sécurité
Gestion des alertes gouvernementales
Coordonnateur Sectoriel en Gestion des Incidents
Chargé de projets - Télécom
Coordonnateur Sectoriel en Gestion des Incidents
Chargé de projets - Exploitation
Supporte
Détenteurs d'actifs
Supporte
Utilisateurs d'actifs

3. Rôles et responsabilités

3.1 Dirigeant de l'établissement (Recteur)

Le chef d'établissement est le premier responsable de la sécurité de l'information à l'UQAC. À ce titre, il doit s'assurer du respect des lois et des règles en sécurité de l'information déterminés par le Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques. Il doit s'assurer que les divers éléments structurants soient en place, mis à jour et déposés au DRI du MEESR.

- Assure le suivi de la mise en œuvre des recommandations émises par le Conseil du trésor ou par le dirigeant principal de l'information ou par le dirigeant réseau;
- Examine les plans d'action de l'UQAC et donne des conseils quant aux modifications à y apporter.

3.2 Responsable de la sécurité de l'information (RSI)

Les rôles et responsabilités présentés ci-dessous pour le RSI sont similaires à ceux du ROSI-réseaux. Le RSI a notamment comme rôle :

- Collaborer avec le ROSI-réseaux, le COSI-réseaux et le COGI-réseaux du MEESR dans la mise en œuvre des orientations gouvernementales en sécurité de l'information;
- D'assister le recteur de l'UQAC en ce qui a trait à la détermination des orientations stratégiques et des priorités d'intervention de son organisation en sécurité de l'information;
- D'assurer l'arrimage de toutes les préoccupations en matière de sécurité de l'information de l'UQAC, incluant celles associées aux technologies de l'information;
- De coordonner le comité de sécurité de l'UQAC.

3.3 Comité de sécurité de l'information

Le comité chargé de la sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information à l'UQAC.

Plus particulièrement, il :

- Examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'UQAC, 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'UQAC.

Ce comité est présidé par le RSI. Il nécessite notamment, la participation des ressources suivantes ainsi que de toute personne jugée pertinente, sur invitation du RSI.

- RSI (Vice-recteur aux affaires administratives)
- Affaires juridiques
- Archiviste
- Conseillers organisationnels en sécurité de l'information (COSI)
- Direction des communications et des relations publiques
- Direction du Service des ressources humaines
- Représentant des professeurs
- Registraire

- Direction du Service des technologies de l'information

3.3.1 Comité de crise

En cas d'incident critique de sécurité de l'information, le comité de crise est le groupe décisionnel appelé à intervenir. À ce titre, il a pour rôle, principalement :

- D'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information;
- D'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants;
- De décider du déploiement ou non des plans de continuité des services;
- De proposer des orientations à suivre ou des actions à prendre en cas de sinistre;
- De formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation;
- De communiquer avec les médias.

Ce comité de crise est présidé par le RSI. Il nécessite notamment, la participation des ressources suivantes ainsi que de toute personne jugée pertinente, sur invitation du RSI.

- RSI (Vice-recteur aux affaires administratives)
- Affaires juridiques
- Responsable de la sécurité physique
- Conseillers organisationnels en sécurité de l'information (COSI)
- Coordonnateur sectoriels en gestion des incidents
- Direction des communications et des relations publiques
- Responsable de l'exploitation et télécommunications
- Direction du Service des technologies de l'information

3.4 Responsable de la gestion des technologies de l'information (RGTI)

Le responsable de la gestion des technologies de l'information apporte son soutien au RSI, notamment en ce qui concerne la mise en œuvre des mesures de sécurité, la mise en place des processus officiels de sécurité de l'information et la participation du Service des technologies de l'information au réseau d'alerte.

- Gère la mise en œuvre des mesures permettant d'assurer la sécurité de l'information numérique détenue par son organisation;
- Coordonne la mise en œuvre des processus officiels de sécurité de l'information, tels que la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- Coordonne l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information.

3.5 Le conseiller organisationnel en sécurité de l'information (COSI)

Le conseiller organisationnel en sécurité de l'information apporte son soutien au RSI, 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, il :

- 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'actions de sécurité de l'information de l'UQAC;

- S'assure de l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans le cadre des ententes de service et des contrats;
- Assiste les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information;
- Élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
- Élabore la mise en œuvre des processus officiels de sécurité de l'information tels que la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- Tient à jour le registre d'autorité de la sécurité de l'information;
- Participe au réseau des conseillers organisationnels en sécurité de l'information;
- Propose au RGTI des orientations, des plans d'action et des bilans;
- Assure la coordination et la réalisation de projets de sécurité de l'information.

3.6 Coordonnateurs sectoriel en gestion des incidents (CSGI)

Collaborant étroitement avec le COGI-réseaux du MEESR, les CSGI des établissements des réseaux de l'éducation agissent au niveau tactique et opérationnel et apportent leur soutien au RSI de l'UQAC et au COSI, notamment au niveau de la gestion des incidents et des risques en SI. Il est l'interlocuteur officiel de l'UQAC auprès du CERT/AQ. Pour remplir son rôle, il a comme responsabilités :

- De collaborer auprès du COSI et du RSI de l'UQAC à l'élaboration des divers éléments stratégiques et tactiques ;
- De participer avec le COGI-réseaux au processus gouvernemental de gestion des incidents, et au réseau d'alerte gouvernemental coordonné par le CERT/AQ;
- D'élaborer et mettre en œuvre, avec le soutien du COGI-réseaux, un processus formel de gestion et de déclaration des incidents de son organisme (sectoriel) incluant un registre des incidents de son organisation;
- De mettre en œuvre les stratégies de réactions appropriées pour l'UQAC lors d'incident, de concert avec le COGI-réseaux du MEESR;
- De contribuer aux analyses de risques de sécurité de l'information, d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées pour l'UQAC;
- De contribuer à l'auto-évaluation de la sécurité des systèmes informatiques et des réseaux informatiques de l'UQAC, notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risques;
- D'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications mis en place à l'UQAC;
- De maintenir une veille continue sur les risques, les menaces et les vulnérabilités, notamment en assistant hebdomadairement aux téléconférences du CERT/AQ.

3.7 Détenteurs de l'information

Les détenteurs de l'information désignés par l'UQAC sont notamment chargés :

- De catégoriser l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité;
- De participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans;

- De veiller 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;
- De supporter les utilisateurs d'actifs concernant les mesures de sécurité mises en place.

3.8 Le gestionnaire

Le gestionnaire est responsable de la mise en œuvre, auprès du personnel relevant de son autorité, des dispositions de la politique de sécurité de l'information. Il doit principalement :

- Informer son personnel des dispositions de la politique sur la sécurité de l'information et de toute directive, de tout standard et de toute procédure en vigueur en matière de sécurité de l'information, ainsi que des modalités liées à leur mise en œuvre, et le sensibiliser à la nécessité de s'y conformer;
- S'assurer que les actifs informationnels mis à la disposition de son personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
- S'assurer que la sécurité de l'information est prise en compte dans tout contrat de service attribué par son unité administrative et voir à ce que tout consultant, partenaire ou fournisseur s'engagent à respecter et respectent les règles de sécurité de l'information de l'UQAC.

3.9 Responsable de l'accès à l'information et de la protection des renseignements personnels

Le responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de *la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1)*. À ce titre, il :

- Communique au ROSI les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible;
- 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 incidents de sécurité de l'information.

3.10 Responsable de la gestion documentaire

Le responsable de la gestion documentaire doit, notamment :

- Collaborer à la conception des systèmes informatiques, administratifs ou autres et s'assurer 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;
- Collaborer étroitement avec les détenteurs de l'information, le responsable ou le conseiller organisationnel en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

3.11 Responsable du développement ou de l'acquisition de systèmes d'information

Le responsable du développement ou de l'acquisition de systèmes d'information conçoit, réalise et documente les fonctionnalités de sécurité de l'information. Ces

fonctionnalités peuvent inclure celles liées au respect des exigences légales de protection des renseignements personnels à intégrer aux systèmes d'information. Le responsable s'assure également du bon fonctionnement de ces systèmes.

3.12 Responsable de la sécurité physique

Le responsable de la sécurité physique 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. Plus particulièrement, le responsable de la sécurité physique :

- Conçoit et met en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de l'UQAC;
- Élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

4. Mise à jour

La révision du cadre de gestion doit être effectuée au besoin et minimalement aux trois (3) ans par le responsable de la sécurité de l'information.

5. Dispositions finales

Le présent cadre de gestion de la sécurité de l'information entre en vigueur à la date de son approbation par le Conseil d'administration.