UNIVERSITÉ DU QUÉBEC
EN ABITIBI-TÉMISCAMINGUE

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

ADOPTÉE 438-CA-4969 (2022-02-08)

Note : Afin de limiter l'impact des biais et des préjugés qui peuvent se retrouver dans les documents publiés de l'Université et reconnaître la diversité des membres de la communauté universitaire, la présente politique intègre les principes de la rédaction épicène.

PRÉAMBULE :

En tant qu'organisme public, l'Université du Québec en Abitibi-Témiscamingue (ci-après « Université » ou « UQAT ») a l'obligation de protéger l'information stratégique et confidentielle qu'elle collecte et détient, incluant les données recueillies sur toute personne, et d'en garantir la disponibilité, l'intégrité et la confidentialité pour toute la durée justifiant sa conservation et pour laquelle des contraintes de diffusion s'appliquent. Cette information comprend notamment des renseignements personnels des membres de la Communauté universitaire et des informations sujettes à des droits de propriété intellectuelle, incluant le secret commercial. Elle inclut également toutes les données, informations ou documents jugés stratégiques pour l'Université ou pour ses partenaires, peu importe que ceux-ci aient été créés ou reçus de différentes sources.

La responsabilité de protection de l'UQAT inclut, sans s'y limiter, la gestion de l'accès à cette information confidentielle et stratégique aux seules personnes chargées d'intervenir qui y sont autorisées dans le cadre de leurs fonctions. Elle s'applique à la fois aux documents papier et aux données numériques sous la garde de l'Université, à l'inclusion des données entreposées dans les plateformes technologiques qu'elle met à la disposition des membres de la Communauté universitaire (par exemple : l'environnement Microsoft 365) et dans les systèmes qu'elle exploite (par exemple : Gesta ; SAFIRH ; Moodle).

La présente Politique a été adoptée en application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* et de la *Directive gouvernementale sur la sécurité de l'information* émise par le Conseil du trésor. Elle vise à renforcer le cadre de gouvernance de la sécurité de l'information de l'Université en établissant des mesures et des contrôles rationnels visant à préserver la confidentialité, l'intégrité et l'accessibilité de l'information qui lui appartient ou sous sa responsabilité. Ces mesures et contrôles tiennent compte de la valeur de cette information et incluent aussi bien les modalités d'accès physique à un local ou à une unité de rangement contenant des documents qu'à l'utilisation de tout outil technologique exploité par l'établissement.

En clarifiant les rôles et responsabilités de l'ensemble des membres de la Communauté universitaire à l'égard de la sécurité de l'information, cette Politique permet à l'Université de respecter les lois, directives et pratiques émises par les instances gouvernementales concernées. Ce faisant, elle participe à la réduction et à la mitigation des risques pouvant affecter l'information confidentielle ou stratégique dont l'UQAT a la responsabilité et contribue à la poursuite de sa mission d'enseignement et de recherche.

En se basant par ailleurs sur le fait que l'environnement technologique est en évolution constante, et en considérant le facteur humain comme élément clé du succès d'un programme de sécurité de l'information, cette Politique vise à intégrer les dimensions de communication, de sensibilisation et de formation aux processus formels de sécurité de l'information.

ARTICLE 1 — DÉFINITIONS

Actif informationnel : Tout document et toutes données, incluant des courriels institutionnels et des données de recherche, ainsi que tout système permettant leur consultation et leur exploitation, les logiciels, systèmes d'exploitation et équipements dans lesquels se trouvent de l'information, peu importe le support (papier, électronique ou autre).

Voici quelques exemples d'actifs informationnels :

- Un dossier physique (papier) sur une personne employée ou étudiante ;
- Les boîtes courriel gérées par l'UQAT ;
- Un système d'information (ex. Gesta) ;
- Une plateforme d'enseignement (ex. Moodle) ;
- Un équipement informatique appartenant à l'UQAT (ex. ordinateur, tablette, serveur) ;
- Le contenu des serveurs de fichiers (exemple : documents appartenant à une entité, à un ou une membre du corps professoral ou de la Communauté étudiante).

L'UQAT est responsable d'assurer la sécurité des actifs informationnels sous sa responsabilité, qu'elle en soit propriétaire ou non.

Cadre de gouvernance en gestion et sécurité de l'information (ci-après « Cadre de gouvernance GSI ») : Comprend le contenu de la présente Politique, le Plan d'action en sécurité de l'information, le Plan des mesures d'urgence de l'Université, les différentes procédures, directives et guides ou autres documents de même nature qui en découlent (voir l'article 4), de même que les procédures de gestion des incidents spécifiques à la sécurité de l'information.

Le Cadre de gouvernance GSI vise à renforcer les systèmes de contrôles internes en offrant une assurance raisonnable de conformité en regard des lois et directives gouvernementales, ainsi qu'aux autres besoins de l'Université en matière de gestion des risques associés à la protection de l'information. Il constitue ainsi un moyen d'ajuster le niveau de risque par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information, selon un effort proportionnel à la sensibilité de cette information et aux effets potentiels envisagés en cas d'incident.

Confidentialité : (voir information confidentielle).

Conseil d'administration : Conseil d'administration de l'Université.

Comité de gouvernance en gestion et sécurité de l'information (ci-après « Comité GSI ») : Comité composé des cadres supérieures et des cadres supérieurs de l'établissement, tel que présenté à l'Annexe 1.

Communauté étudiante : Ensemble de la population étudiante de l'Université (active ou non).

Communauté universitaire : Comprend, au sens large, les membres du personnel, incluant les membres du corps professoral ; le personnel chargé de cours ; les groupes, équipes, unités, centres et chaires de recherche ; les membres des conseils de modules et des comités de programmes d'études de 1er cycle ou d'études de cycles supérieurs ; la communauté étudiante (active ou non). Sont également considérés comme des membres de la Communauté universitaire le personnel et les membres de la Commission des études et du Conseil d'administration ; les membres de tous les comités créés par l'une ou l'autre des instances administratives et académiques de l'Université ; les organismes externes et personnes physiques qui exploitent l'infrastructure logicielle de l'UQAT : notamment, l'Association générale étudiante de l'UQAT (AGEUQAT), les diplômées et diplômés de l'UQAT, les syndicats de l'Université, la Fondation de l'UQAT, les retraitées et les retraités de l'UQAT, les membres de l'Association des retraités de l'UQAT (ARUQAT), la Société de l'eau souterraine de l'Abitibi-Témiscamingue (SESAT) et la Société Immobilière de l'Université du Québec (SIUQ).

Cycle de vie de l'information : Ensemble des étapes que franchit une information, qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'Université au sens la *Loi sur les archives*.

Détenteur d'actifs informationnels : Membre de la Communauté universitaire qui détient des responsabilités ou des droits de propriété (notamment de propriété intellectuelle) sur des documents, informations ou données entreposées sur les systèmes informatiques de l'UQAT. La direction de chaque entité et les chercheuses et chercheurs, notamment, sont considérés comme détentrices et détenteurs des actifs informationnels sous leur responsabilité, à l'inclusion des données de recherche qu'ils collectent, traitent et analysent.

Direction de l'entité : Membre du personnel-cadre responsable d'une structure administrative de l'Université.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Document : Est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle y 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.

Données : Représentation de faits sous forme de textes, de chiffres, de graphiques, d'images, de sons ou de vidéos[1]. Par exemple, le numéro d'assurance sociale (NAS) d'un ou d'une membre du personnel ou le code permanent d'un étudiant ou d'une étudiante constituent des données.

[1] Définition tirée de la page *Les données, l'information statistique et les statistiques* (Statistiques Canada, 2022).

Entité : Instance administrative ou académique de l'Université.

Incident de sécurité : Problématique impliquant une atteinte potentielle à la disponibilité, l'intégrité ou la confidentialité d'un ou de plusieurs documents ou de tout autre actif informationnel (par exemple le contenu d'une boîte courriel). Les incidents incluent, sans s'y limiter, la réception de courriels suspects, la détection de virus et la transmission de données à une personne non autorisée. Les incidents de sécurité de l'information à portée gouvernementale sont quant à eux des incidents pouvant entraîner des conséquences envers la prestation de services indispensables à la Communauté universitaire. Cette atteinte doit avoir un impact présumé ou avéré sur la vie, la santé et le bien-être des personnes ainsi que sur le respect de leurs droits fondamentaux, de la protection de leurs renseignements personnels, de leur vie privée, ainsi qu'à l'image du gouvernement.

Information : Renseignements consignés sur un support (papier, électronique, etc.) et visant à transmettre des connaissances[2]. L'information est constituée d'un ensemble de données mises en contexte.

Information accessible : Propriété d'une information d'être disponible en temps voulu et de la manière requise pour une personne dûment autorisée.

Information confidentielle : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées ou autorisées.

Intégrité : Propriété d'une donnée ou d'un document de ne subir aucune altération ou destruction.

Loi : *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03).

Politique de sécurité ; Politique : Réfère à la présente Politique.

Propriété intellectuelle : La propriété intellectuelle est un régime juridique qui vise à reconnaître le mérite d'une réalisation en accordant à son ou ses auteurs ou autrices le droit exclusif de diffusion et d'exploitation de celle-ci. La propriété intellectuelle s'exprime de diverses façons, dont le droit d'auteur qui touche principalement le domaine littéraire, scientifique ou artistique, et le brevet d'invention qui concerne surtout des productions de type industriel. Pour plus d'informations, se référer à la *Politique et règles en matière de propriété intellectuelle de l'UQAT*.

Université ou **UQAT** : Université du Québec en Abitibi-Témiscamingue.

Registre d'autorité de la sécurité de l'information : Registre dans lequel sont notamment consignés les noms des détentrices et détenteurs de l'information, les systèmes qui leur sont assignés ainsi que les rôles et les responsabilités des principales intervenantes et principaux intervenants en sécurité de l'information. Ce registre inclut la catégorisation des actifs informationnels.

[2] Définition tirée du *Thésaurus de l'activité gouvernementale* (Gouvernement du Québec, 2022).

Renseignements confidentiels : Renseignements concernant une tierce partie (personne physique ou morale) et ne pouvant être divulgués sans son consentement au risque de lui causer un préjudice physique, moral, financier ou stratégique. Sont notamment considérés comme confidentiels, les renseignements personnels ainsi que tout renseignement dont la divulgation à des personnes non autorisées à les recevoir aurait une ou plusieurs incidences sur : la bonne conduite des affaires ; la protection des membres de la Communauté universitaire ; le positionnement stratégique de l'Université ; les organismes, établissements, partenaires financiers et industriels et les particuliers entretenant des liens avec elle.

Risque acceptable : Risque relatif à un ou plusieurs actifs ne nécessitant pas la prise de mesures supplémentaires d'atténuation, vu la faible vraisemblance d'occurrence ou les impacts potentiels jugés non critiques.

Sécurité de l'information : Ensemble de principes et pratiques relatives à la protection des données, quel que soit leur support (papier ou numérique). La sécurité de l'information inclut donc la cybersécurité, laquelle concerne plus spécifiquement la protection des données numériques, des appareils et des réseaux contre des cybermenaces et des acteurs malveillants.

Utilisatrice ou utilisateur : Toute personne qui fait usage des actifs informationnels visés par la présente Politique.

ARTICLE 2 — OBJECTIFS DE LA POLITIQUE

La présente Politique a pour objectif d'affirmer l'engagement de l'UQAT de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication, tout au long de son cycle de vie. Elle soutient également la mise en œuvre du Cadre de gouvernance GSI de l'Université. Plus précisément, l'Université doit veiller à :

- La disponibilité de l'information, de façon à ce qu'elle soit accessible en temps voulu et de manière appropriée pour les personnes autorisées ;
- L'intégrité de l'information, de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans avoir obtenu au préalable l'autorisation de l'entité responsable, et que le support de cette information lui procure la stabilité et la pérennité attendues ;
- La confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, peu importe le support qui la contient, et à plus forte raison si celle-ci comporte des renseignements personnels ;
- L'accessibilité à un environnement technologique favorisant notamment la qualité des activités d'apprentissage, la conduite des travaux de recherche et la poursuite des activités administratives dans le respect des meilleures pratiques de la sécurité de l'information ;
- L'attribution claire des responsabilités et la mise en place d'un processus de saine gestion interne de la sécurité de l'information soutenant les activités de planification, d'application des mesures requises et d'audit des pratiques aux fins de reddition de compte.

ARTICLE 3 — CHAMP D'APPLICATION

Cette Politique s'adresse aux membres de la Communauté universitaire, de même qu'à toute personne externe, physique ou morale, dûment autorisée à obtenir accès à un ou plusieurs actifs informationnels de l'Université.

La Politique concerne tous les actifs informationnels sous la responsabilité de l'UQAT, que ces actifs soient collectés et/ou lui appartiennent et qu'ils soient détenus et/ou utilisés par elle ou par un tiers, au bénéfice et au nom de l'Université.

ARTICLE 4 — CADRE LÉGAL ET ADMINISTRATIF

La Politique de sécurité s'inscrit dans un contexte principalement régi par le cadre légal suivant :

- La Charte des droits et libertés de la personne (RLRQ, c C-12) ;
- Le Code civil du Québec (RLRQ, c CCQ-1991) ;
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c G-1.03) ;
- La Loi concernant le cadre juridique des technologies et l'information (RLRQ, c C-1.1) ;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c A-2.1) ;
- La Loi sur les archives (RLRQ, c A-21.1) ;
- Le Code criminel (LRC 1985, c C-46) ;
- La Loi sur le droit d'auteur (LRC 1985, c C-42) ;
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics (Gouvernement du Québec — 2010) ;
- La Directive gouvernementale sur la sécurité de l'information (Décret 1514-2021 du 8 décembre 2021) ;
- L'Énoncé de Politique des trois conseils : Éthique de la recherche avec des êtres humains (CRSH, CRSNG et IRSC, 2018) ;
- La Politique gouvernementale de cybersécurité (SCT, mars 2020) ;
- La Politique des trois organismes sur la gestion des données de recherche (CRSH, CRSNG et IRSC, 2021).

La Politique de sécurité encadre principalement les Politiques, directives et règlements de l'Université suivants :

- Règlement 6 — Archives et gestion documentaire ;
- Politique de gestion des risques ;
- Politique d'utilisation du courrier électronique, d'Internet, des médias sociaux et des ressources technologiques de l'UQAT ;
- Politique sur l'accès aux documents et sur la protection des renseignements personnels ;
- Politique et règles en matière de propriété intellectuelle ;
- Politique et procédure relative à l'acquisition et à l'utilisation des logiciels ;
- Procédure visant à faciliter la divulgation d'actes répréhensibles commis à l'égard de l'UQAT ;
- Stratégie institutionnelle de gestion des données de recherche de l'UQAT *(en cours d'élaboration)* ;
- Directive en matière d'accès *(en cours d'élaboration)*.

ARTICLE 5 — PRINCIPES DIRECTEURS

Les principes directeurs guidant les actions de l'Université en matière de sécurité de l'information sont les suivants :

a) La reconnaissance de l'importance d'assurer la sécurité de l'information en fonction de sa valeur ;

b) La protection adéquate de l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction (le niveau de sécurité à appliquer pouvant varier au cours du cycle de vie d'un document ou d'un ensemble de données) ;

c) L'appui sur les normes de l'industrie et les recommandations du Secrétariat du Conseil du trésor afin de favoriser le déploiement des meilleures pratiques, le recours à des barèmes de comparaison avec des organismes ou établissements similaires et l'assurance du respect des exigences légales et réglementaires ;

d) L'identification continue et la priorisation des risques, dans une perspective de maintien d'un niveau de risque acceptable, en tenant compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques ;

e) La réalisation d'une planification des activités en sécurité de l'information faisant l'objet d'un suivi régulier auprès des instances décisionnelles de l'Université afin d'assurer une saine gouvernance ;

f) L'élaboration et la mise à jour d'un plan de gestion d'incidents de sécurité de l'information, afin de permettre une réaction efficiente en cas d'occurrence d'un évènement et d'assurer le rétablissement des services essentiels à la Communauté universitaire selon un temps déterminé ;

g) Le partage des meilleures pratiques et le maintien d'une collaboration avec le réseau de l'éducation et d'autres organismes publics ;

h) L'établissement d'une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle : chaque individu qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci ;

i) La prise en compte des besoins des utilisateurs lors de la planification, configuration et activation de mesures de sécurité ;

j) L'établissement d'une approche fondée sur la communication, l'accompagnement, la sensibilisation et la formation de la Communauté universitaire aux meilleures pratiques, afin que chaque membre puisse comprendre l'importance d'appliquer les consignes de sécurité demandées, reconnaître les signes d'un incident et agir en conséquence.

ARTICLE 6 — MESURES GÉNÉRALES EN SÉCURITÉ DE L'INFORMATION

L'Université s'engage à prendre les mesures générales suivantes en sécurité de l'information :

6.1 Tenue à jour d'un registre d'autorité de la sécurité de l'information

L'Université reconnaît que ses actifs informationnels, ainsi que tous les actifs informationnels sous sa responsabilité (par exemple, les données de recherche), sont essentiels à ses activités et permettent de réaliser sa mission. De ce fait, ces actifs doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection appliqué aux actifs informationnels doit être établi en fonction de leur importance, de leur confidentialité et des risques d'incident, d'erreur et d'utilisation malveillante auxquels ils sont exposés. Dans cette perspective, l'Université s'engage à dresser et à tenir à jour un registre d'autorité, incluant la localisation des actifs informationnels, la liste des détentrices et détenteurs principaux et des partenaires impliqués dans leur création, la gestion ou la transmission de l'information, ainsi que l'évaluation de leurs niveaux de criticité, afin d'orienter ses actions en matière de prévention, protection et préservation.

6.2 Formalisation du cadre normatif institutionnel

L'Université s'engage à mettre en place des guides, directives, procédures, ou tout autre document de même nature, afin d'assurer la mise en place du Cadre de gouvernance GSI et permettre la traçabilité des actions effectuées sur les actifs informationnels.

6.3 Élaboration d'un plan d'action

L'Université s'engage à mettre en place et tenir à jour un plan d'action pour se conformer aux exigences légales et réglementaires et pour assurer l'amélioration continue de son niveau de maturité organisationnelle en sécurité de l'information.

6.4 Sensibilisation et formation

L'Université s'engage à sensibiliser et à former sur une base régulière les utilisateurs et les utilisatrices à la sécurité des actifs informationnels, à leur rôle et responsabilité en la matière ainsi qu'aux conséquences d'un incident.

6.5 Élaboration et mise à jour d'un plan de gestion des incidents

L'Université s'engage à élaborer et à mettre à jour un Plan de gestion des incidents de sécurité de l'information arrimé à son Plan des mesures d'urgence. Ce Plan doit inclure les plans d'escalade et de relève en cas d'incident afin d'assurer une réaction efficiente lors d'un évènement et d'assurer le rétablissement des services essentiels à la Communauté universitaire selon un temps déterminé.

ARTICLE 7 — RÔLES ET RESPONSABILITÉS EN SÉCURITÉ DE L'INFORMATION

La présente Politique établit les rôles et responsabilités en matière de sécurité de l'information, lesquels sont attribués comme suit :

7.1 Conseil d'administration

- Adopte la Politique et ses modifications ;
- S'assure de la mise en place d'un Cadre de gouvernance GSI ;
- Prend connaissance des redditions de compte qui lui sont présentées ;
- Approuve les orientations organisationnelles en matière de sécurité de l'information ;
- S'assure de l'allocation des budgets, par une analyse des priorités organisationnelles, nécessaires à l'accomplissement des objectifs et des orientations figurant à la Politique.

7.2 Comité GSI

- Recommande l'adoption du plan d'action en sécurité de l'information ;
- Évalue l'efficacité et le rendement du plan d'action en sécurité de l'information ;
- Entérine les recommandations en sécurité de l'information et assure le suivi auprès du Conseil d'administration, au besoin ;

- Approuve le programme de formation et de sensibilisation du personnel en matière de sécurité de l'information ;
- Approuve le Plan des mesures d'urgence de l'Université et les procédures spécifiques associées à la gestion des incidents de sécurité de l'information ;
- Adresse les recommandations nécessaires au comité exécutif en lien avec la présente Politique ;
- Valide le contenu des redditions de comptes à l'intention des instances gouvernementales concernées ;
- Agit à titre de comité de crise en cas d'incident.

7.3 Rectorat

- Participe activement au Comité GSI ;
- Est notifié de tout risque ou incident majeur ayant un impact sur la sécurité de l'information et détermine les orientations organisationnelles pour gérer l'incident ;
- Recommande les orientations organisationnelles en matière de sécurité de l'information ;
- Recommande l'allocation des budgets nécessaires à l'accomplissement des objectifs et des orientations figurant à la Politique.

7.4 Secrétariat général

- Participe activement au Comité GSI ;
- Est notifié de tout risque ou incident majeur ayant un impact sur la sécurité de l'information et détermine les orientations organisationnelles pour gérer l'incident ;
- Adresse les recommandations nécessaires au Conseil d'administration en lien avec la Politique et s'assure de la réalisation de reddition de comptes à son attention ;
- Approuve les directives, procédures, processus et guides découlant de la présente Politique et s'assure de sa communication à l'ensemble des membres de la Communauté universitaire ;
- Recommande l'allocation des budgets nécessaires à l'accomplissement des objectifs et des orientations figurant à la Politique ;
- Agit à titre de responsable organisationnel en sécurité de l'information, incluant le volet de conformité de la gestion des accès, et de chef de la sécurité de l'information organisationnelle ;
- S'assure des révisions périodiques du Cadre de gouvernance GSI ;
- Supervise et oriente le travail de la personne responsable en sécurité de l'information ;
- Désigne les détentrices et détenteurs de l'information et les responsables d'actifs informationnels afin de les inscrire au Registre d'autorité de la sécurité de l'information ;
- S'assure de la réalisation d'un audit de sécurité de l'information, selon une périodicité bisannuelle (minimalement, ou à la suite de tout changement majeur susceptible d'entraîner

des conséquences sur la sécurité de l'information), et en dégage les priorités d'action ainsi que les échéanciers afférents en collaboration avec le Service des technologies de l'information ;

- Est responsable de la gestion des incidents, incluant la mise en place et tenue à jour de procédures spécifiques associées au Plan des mesures d'urgence de l'Université.

7.5 Vice-rectorat aux ressources

- Participe activement au Comité GSI ;
- Recommande l'allocation des budgets nécessaires à l'accomplissement des objectifs et des orientations figurant à la Politique suivant une analyse stratégique de l'ensemble des priorités organisationnelles ;
- Supervise le processus de négociation des cyberassurances et recommande la souscription aux instances décisionnelles de l'Université ;
- S'assure d'intégrer les composantes du plan de gestion des incidents de sécurité de l'information au Plan des mesures d'urgence de l'Université.

7.6 Direction du Service des technologies de l'information

- Participe activement aux groupes de travail découlant du Comité GSI, dont l'équipe tactique en prévention et gestion des incidents ;
- Participe au processus d'élaboration du plan de gestion des incidents et s'assure de communiquer son contenu aux membres de son équipe ;
- S'assure de la mise place des systèmes automatisés de surveillance et de détection proportionnels aux risques à mitiger ;
- Applique les recommandations de sécurité formulées en respect des budgets et des ressources disponibles ;
- S'assure de la réalisation de tests d'intrusion et de vulnérabilité, au minimum sur une base annuelle, ou à la suite d'un changement majeur susceptible d'entraîner des conséquences sur la sécurité de l'information, et en dégage les priorités d'actions et les échéanciers afférents ;
- Favorise l'utilisation des services communs de sécurité de l'information déterminés par le Secrétariat du Conseil du trésor.

7.7 Responsable en sécurité de l'information

- S'assure de la mise en place du Cadre de gestion de la sécurité de l'information et d'un registre d'autorité de la sécurité de l'information ;
- Élabore le plan d'action, coordonne les activités qui y sont prévues et rend compte de l'avancement des tâches prévues dans le cadre des redditions internes et externes prévues ;
- S'assure de la conduite récurrente d'analyse de risques, d'évaluation des besoins et d'anticipation des menaces ;

- Émet des recommandations dictant les principes à adopter en matière de sécurité de l'information, en conformité avec le cadre législatif et réglementaire ;
- Élabore le programme de formation et de sensibilisation à la Communauté universitaire ;
- Participe à la rédaction des directives, procédures, processus et guides découlant de la présente Politique ;
- Prépare et dépose les redditions de comptes et bilans de sécurité de l'information requis par les instances gouvernementales concernées ;
- Rédige et tient à jour le plan de gestion des incidents et le registre des évènements, et s'assure d'en communiquer le contenu aux personnes concernées ;
- Fait partie des groupes de travail découlant du Comité GSI, dont l'équipe tactique en prévention et gestion des incidents ;
- Adresse les recommandations nécessaires au Comité GSI en lien avec la présente Politique ;
- Offre un service-conseil à la Communauté universitaire en matière de sécurité de l'information, notamment lors de l'acquisition de nouveaux outils technologiques ou la gestion de changements technologiques ;
- Déclare au MES, au Rectorat et au Secrétariat général, selon les modalités fixées par ce dernier, les incidents de sécurité de l'information à portée gouvernementale ;
- Déclare au Rectorat et au Secrétariat général les risques en sécurité de l'information, dont ceux à portée gouvernementale ;
- Dépose au Secrétariat général une planification des actions en sécurité de l'information de façon annuelle (incluant priorités d'action et échéanciers afférents découlant des exercices d'audit et tests d'intrusion).

7.8 Service des archives et gestion documentaire

- Constitue et tient à jour la catégorisation des actifs informationnels de l'Université, en collaboration avec les détenteurs et détentrices de ceux-ci ;
- Collabore avec le Service des technologies de l'information, la personne responsable en sécurité de l'information et avec les détenteurs et détentrices d'actifs informationnels pour identifier et localiser ces actifs, et déterminer les meilleures pratiques d'utilisation, de protection et de partage des actifs informationnels compte tenu de leurs niveaux de criticité.

7.9 Détentrices et détenteurs d'actifs informationnels

- S'assurent de l'application de saines pratiques de gestion et de manipulation de l'information au sein de leur équipe ;
- Évaluent la disponibilité, l'intégrité et la confidentialité des actifs sous leur responsabilité lors de la mise à jour de la catégorisation des actifs informationnels, en collaboration avec le Service des archives et gestion documentaire ;

- Informent le Service des archives et gestion documentaire de tout changement à leurs processus d'affaires ou de tout ajout d'actifs informationnels qui requièrent une mise à jour au registre d'autorité de la sécurité de l'information ;
- Déterminent les droits d'accès spécifiques associés à ces actifs, conformément à l'évaluation de la criticité des informations qui y sont contenues et aux fonctions officielles des personnes désignées pour y accéder et sur la base des lignes directrices fournies par le Secrétariat général ;
- Collaborent avec le Service des technologies de l'information pour trouver les périodes les plus appropriées pour les rehaussements et les mises à jour critiques ;
- Signalent immédiatement tout acte dont ils ont connaissance et qu'ils estiment susceptible de constituer une violation réelle ou présumée aux règles de sécurité, ainsi que toute anomalie ou tout incident pouvant nuire à la protection des actifs informationnels sous leur responsabilité :
    - En contactant directement le *819-762-0971 poste 2525 ;*
    - En suivant les instructions fournies par le personnel du Service des technologies de l'information et/ou du Secrétariat général ;
- Suivent les directives établies au moment d'acquérir ou d'utiliser tout nouveau logiciel.

7.10 Utilisatrices et utilisateurs

- Prennent connaissance de la présente Politique, des directives, des procédures et autres lignes de conduite en découlant, et veillent à observer en tout temps leurs obligations en regard de ces documents ;
- Utilisent les actifs informationnels mis à leur disposition dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, en se limitant aux fins auxquelles ils sont destinés et en respectant les restrictions de diffusion liées à leur niveau de confidentialité ;
- Respectent les mesures de sécurité mises en place sur leur poste de travail ainsi que lors de la manipulation de tout équipement ou document contenant des données à protéger ;
- Se conforment aux exigences légales et aux procédures organisationnelles portant sur la manipulation et l'utilisation de tout actif informationnel contenant des renseignements personnels ou sujet à l'application de droits de propriété intellectuelle ;
- Consentent, par l'utilisation des outils et infrastructures technologiques de l'UQAT, à ce qu'une surveillance automatisée soit effectuée afin de mitiger les risques en sécurité de l'information afférents ;
- Participent à tous les exercices et formations identifiés comme obligatoires par l'Université ;
- Lors de séjour de déplacement à l'international, notamment dans le cadre d'activités de recherche, observent les pratiques recommandées par le Gouvernement du Canada et contactent l'équipe de Sécurité de l'information du Secrétariat général pour toutes références utiles, au besoin ;

- Signalent immédiatement tout acte dont ils ont connaissance et qu'ils estiment susceptible de constituer une violation réelle ou présumée aux règles de sécurité, ainsi que toute anomalie ou tout incident pouvant nuire à la protection des actifs informationnels sous leur responsabilité :
    - En contactant directement le *819-762-0971 poste 2525 ;*
    - En suivant les instructions fournies par le personnel du Service des technologies de l'information et/ou du Secrétariat général ;
- Remettent, au moment de leur départ de l'Université, l'ensemble des actifs informationnels (incluant l'équipement informatique ou téléphonique, l'information sur support électronique ou papier, ou autres) appartenant à l'UQAT et mis à leur disposition dans le cadre de leurs fonctions.

7.11 Signataires des contrats

En plus de leurs responsabilités d'utilisatrices et d'utilisateurs, et le cas échéant, étant des personnes détenant des actifs informationnels, les signataires des contrats :

- S'assurent, en collaboration avec le Secrétariat général, que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires, stipulent des clauses garantissant le respect des exigences de sécurité de l'information ;
- S'assurent, avant l'acquisition d'une nouvelle plateforme technologique, qu'une validation de sécurité et de conformité de celle-ci ait été préalablement effectuée par le Secrétariat général.

ARTICLE 8 — SANCTIONS

Lorsqu'une utilisatrice ou un utilisateur contrevient à la présente Politique ou aux directives en découlant, cette personne s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats. Dans le cas où l'utilisatrice ou l'utilisateur en défaut est une personne étudiante, ces mesures incluent toute autre sanction pouvant être appliquée en vertu des règlements et politiques les encadrant.

L'Université peut transmettre à toute autorité judiciaire, les renseignements colligés qui portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise.

ARTICLE 9 — DISPOSITIONS FINALES

a) La présente Politique entre en vigueur à la date de son adoption par le Conseil d'administration ;

b) La personne occupant la fonction de secrétaire générale ou de secrétaire général s'assure de la mise en œuvre des dispositions de la présente Politique et de ses directives ;

c) La présente Politique doit être révisée à l'occasion de changements qui pourraient l'affecter ;

d) La présente Politique fait partie du Cadre de gestion de la sécurité de l'information. Les obligations qui en découlent peuvent être précisées dans des directives, procédures, guides ou documents de même nature.

ANNEXE 1 – Composition du comité GSI et des groupes de travail

NOTE : Les personnes participantes identifiées à l'intérieur des équipes de travail constituent un noyau de base. Selon la nature des dossiers à traiter, d'autres personnes peuvent être appelées à intégrer l'une ou l'autre de ces équipes.

Comité de gouvernance en gestion et sécurité de l'information (Comité GSI)

- Personnes participantes : Cadres supérieures et cadres supérieurs

Coordination assurée par la personne responsable en sécurité de l'information

Équipe de travail GSI

- Suivi du plan d'action, du registre des risques et du Registre d'autorité de la sécurité de l'information
- Coordination de la mise en œuvre des livrables
- Identification et analyse de nouveaux risques

Personnes participantes :

- Direction du Service des technologies de l'information
- Employé responsable de la sécurité opérationnelle au Service des technologies de l'information
- Responsable en sécurité de l'information
- Secrétaire générale, au besoin
- Archiviste, au besoin

Équipe de gestion des processus et politiques

- Identification des exigences légales, réglementaires et métier
- Établissement de politiques et de mécanismes de contrôle

Personnes participantes cooptées au besoin:

- Porte-parole du Service des ressources humaines
- Porte-parole du Bureau du registraire
- Porte-parole du vice-rectorat à l'enseignement, à la recherche et à la création
- Porte-parole de la Table de Développements numériques
- Porte-parole du Service des finances

Équipe de gestion de la conformité

- Maintien de l'inventaire du cadre légal et réglementaire
- Validation des priorités et des niveaux d'impacts en matière de protection des renseignements personnels
- Gestion des audits

Personnes participantes :

- Secrétaire générale ou secrétaire général
- Conseillère juridique ou conseiller juridique
- Administratrice ou administrateur – Volet gestion des risques

Équipe tactique de prévention et gestion des incidents

- Élaboration des scénarios d'escalade et des plans de relève en cas d'incident
- Coordination des actions à prendre en cas d'événement

Personnes participantes :

- Direction du Service des technologies de l'information
- Responsable en sécurité de l'information
- Employé responsable de la sécurité opérationnelle au Service des technologies de l'information