UQÀM | Université du Québec à Montréal

Politique sur la sécurité de l'information

Dernière mise à jour :
18 juin 2026

Responsable de l’application	Vice-recteur aux Systèmes d’information
Autorité compétente	Conseil d’administration
Signature	S.O.
Date d’approbation	18 juin 2026
Date d’entrée en vigueur	18 juin 2026
Date de la dernière modification	
Le texte que vous consultez est une codification administrative des Politiques de l’UQAM. Leur version officielle est contenue dans les résolutions adoptées par le Conseil d’administration.	

Table des matières

1. Préambule

L'Université du Québec à Montréal (ci-après l'« Université ») reconnaît que les systèmes d'information sur lesquels elle s'appuie constituent des actifs essentiels à la réalisation de sa mission. Ces systèmes permettent la gestion, le traitement et la communication d'informations cruciales pour ses activités. Par conséquent, l'Université souhaite mettre en place un cadre de gouvernance en sécurité de l'information qui tienne compte des exigences législatives et réglementaires en vigueur, et qui s'inspire des meilleures pratiques en la matière.

Dans le respect de la liberté académique, de la vie privée et de la confidentialité des renseignements personnels des membres de la communauté, les objectifs de la présente politique sont les suivants :

a) protéger les systèmes d'information : assurer leur défense contre les menaces internes, externes et émergentes;

b) favoriser une utilisation responsable et sécuritaire : encourager les personnes membres de la communauté universitaire à l'utilisation sécuritaire, responsable et éthique des systèmes d'information et des données qu'ils supportent;

c) renforcer le développement des compétences et la sensibilisation : informer et former les membres de la communauté universitaire sur les enjeux et les meilleures pratiques en sécurité de l'information;

d) gérer les risques : identifier, analyser, évaluer et atténuer les risques associés aux systèmes d'information, notamment en matière de confidentialité, d'intégrité et de disponibilité des données.

2. Objet

La présente politique définit les principes directeurs orientant les pratiques à adopter pour assurer la sécurité des systèmes d'information de l'Université. Elle vise à préserver la disponibilité et l'intégrité de ces systèmes, et à protéger les données qu'ils supportent des incidents de sécurité tels que la fraude, les fuites d'information, les attaques informatiques, les erreurs accidentelles, les actions délibérées et les atteintes à la vie privée.

Elle détermine également les rôles et les responsabilités de chaque intervenante, intervenant en matière de sécurité des systèmes d'information.

Cette politique s'inscrit dans un cadre institutionnel de gouvernance de l'information, lequel inclut la Politique n° 11 sur la gestion de l'information et des archives et la Directive sur le traitement et la protection des renseignements personnels.

3. Champ d'application

La présente politique concerne tous les systèmes d'information détenus par l'Université. Elle s'applique à toute la communauté universitaire ainsi qu'aux personnes physiques et morales

externes détenant un système d'information pour l'Université. Pour plus de clarté, toute personne appelée à utiliser, gérer, exploiter ou traiter les systèmes d'information de l'Université doit respecter la présente politique.

4. Cadre juridique

La présente politique est élaborée en tenant compte notamment du cadre juridique suivant :

a) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c. A-2.1;
b) Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c. G-1.03 (la « LGGRI »);
c) Loi concernant le cadre juridique des technologies de l'information, RLRQ c. C-1.1;
d) Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c. G-1.03, r. 1;
e) Politique gouvernementale de cybersécurité;
f) Directive gouvernementale sur la sécurité de l'information;
g) Arrêté ministériel n° 2024-05 concernant le Modèle de classification de sécurité des données numériques gouvernementales.

5. Définitions

Aux fins de la présente politique, les termes suivants se définissent comme suit :

a) classification de sécurité : processus permettant de déterminer le niveau de criticité des systèmes d'information, compte tenu du préjudice que peut engendrer un bris de disponibilité ou d'intégrité de ces actifs sur l'Université, sur sa communauté ou sur des tiers. Le niveau de criticité est évalué en fonction notamment de la catégorisation de l'information qui est supportée par le système d'information, comme le prévoit la Politique nº 11 sur la gestion de l'information et des archives;

b) niveau de classification de sécurité : niveau attribué à la suite du processus de classification de sécurité. Les mesures de protection à mettre en place doivent être proportionnelles au niveau de classification du système d'information et aux risques encourus;

c) donnée : représentation isolée de caractères ou de symboles exprimée sous une forme permettant leur traitement par des moyens technologiques;

d) identité : ensemble des attributs permettant de représenter de manière unique une personne ou toute autre entité dans un système d'information;

e) incident de sécurité informatique : événement de sécurité qui compromet, ou pourrait compromettre, la confidentialité, la disponibilité ou l'intégrité d'une information ou d'un système d'information, ou la continuité de service d'une organisation;

f) information : ensemble intelligible de mots, de sons, d'images ou de données contextualisées;

g) gestionnaire : cadre supérieure, cadre supérieur, cadre, doyenne, doyen;

h) niveau d'impact : traduit l'importance des conséquences qu'un incident de sécurité informatique peut avoir sur l'Université, sa communauté ou des tiers;

i) personne administratrice d'un système d'information : toute personne qui configure, gère techniquement un système d'information et en assure la maintenance, en tout ou en partie;

j) personne exploitant un système d'information : toute personne qui gère les accès des personnes utilisatrices à un système d'information;

k) personne utilisatrice d'un système d'information : toute personne à qui est accordé l'accès à un système d'information;

l) plan de reprise après sinistre : plan dans lequel sont prévues les différentes étapes pour rétablir, dans les meilleurs délais, la disponibilité des systèmes d'information soutenant les processus d'affaires critiques de l'Université à la suite d'un sinistre ou d'une interruption majeure;

m) responsable d'un système d'information : toute personne désignée pour superviser la gestion, l'exploitation et l'évolution d'un système d'information;

n) système d'information : ensemble organisé de ressources technologiques utilisé pour traiter, stocker, transmettre ou diffuser de l'information. Cette expression comprend notamment : logiciels et programmes, ordinateur fixe, ordinateur portable, réseau filaire et sans fil, serveur, système téléphonique, appareils mobiles (p. ex. : tablette, cellulaire, etc.), imprimante et autres périphériques, support de données et tout autre outil informatique, incluant les services externalisés (p. ex. : Saas, IaaS, PaaS).

6. Rôles et responsabilités

6.1 Conseil d'administration

Le Conseil d'administration est le dirigeant de l'organisme au sens de l'article 5.1 de la LGGRI. Il établit le cadre de gouvernance de la sécurité de l'information en adoptant la présente politique et ses modifications. Il désigne les personnes répondantes en matière de sécurité de l'information, conformément aux exigences applicables aux organismes publics. Il se tient informé des enjeux critiques de sécurité de l'information susceptibles d'avoir un impact sur la mission, les activités, ou l'atteinte des objectifs stratégiques de l'Université.

6.2 Comité d'audit

Le Comité d'audit assiste le Conseil d'administration dans l'exercice de ses responsabilités de surveillance en matière de sécurité de l'information. À ce titre, il est informé de toute modification apportée au cadre normatif institutionnel de la sécurité de l'information et reçoit annuellement :

- une présentation sur l'évaluation de la posture de l'Université en matière de sécurité de l'information et sur le plan d'action associé;

- une présentation du bilan annuel de la sécurité de l'information, dont il rend compte au Conseil d'administration.

6.3 Vice-rectrice, vice-recteur aux Systèmes d'information

La vice-rectrice, le vice-recteur aux Systèmes d'information est responsable de formuler les grandes orientations en matière de systèmes d'information à l'Université. Elle, il conseille la direction quant à la prise de décision dans ces domaines et agit à titre d'interlocutrice, d'interlocuteur auprès du ministère responsable de l'enseignement supérieur. Elle, il a notamment les responsabilités suivantes :

a) soumettre au Conseil d'administration, pour adoption, la présente politique et par la suite, toute modification qui y sera apportée, sur recommandation de la cheffe, du chef de la sécurité de l'information organisationnelle;

b) informer le Conseil d'administration, pour tout incident de sécurité informatique majeur, de son niveau d'impact, des plans d'action et de reprise après sinistre qui s'y rapportent ainsi que de l'état de leur mise en œuvre;

c) s'assurer du respect des exigences législatives en matière de sécurité des systèmes d'information;

d) s'assurer de l'application et du respect de la présente politique.

6.4 Cheffe, chef de la sécurité de l'information organisationnelle

La cheffe, le chef de la sécurité de l'information organisationnelle (CSIO) est responsable de la gestion globale de la sécurité de l'information au sein de l'Université. La, le CSIO est désigné en vertu de l'article 10 de la Directive gouvernementale sur la sécurité de l'information. À l'Université, cette fonction est exercée par la directrice, le directeur de la sécurité de l'information.

La, le CSIO doit, entre autres choses, veiller à :

a) l'élaboration et au maintien du cadre normatif institutionnel de la sécurité de l'information et soumettre des propositions de modification de la présente politique à la vice-rectrice, au vice-recteur aux Systèmes d'information;

b) présenter au Comité d'audit un bilan annuel de la sécurité de l'information ainsi qu'une évaluation de la posture de sécurité de l'information et le plan d'action qui en découle;

c) étudier les demandes de dérogation aux exigences de sécurité prévues par la présente politique et ses directives associées, et rendre une décision à leur endroit;

d) coordonner la gestion des incidents de sécurité, mettre en place des mesures correctives et assurer un plan de reprise après sinistre en lien avec la continuité des activités;

e) assurer la mise en place des mesures de protection des systèmes d'information et définir les besoins de sécurité nécessaires à assurer leur intégrité et leur disponibilité;

f) définir les critères de sécurité des technologies utilisées et réaliser des évaluations de risques et de vulnérabilités pour les projets impliquant un système d'information détenu par l'Université;

g) fournir des conseils en sécurité des systèmes d'information, sensibiliser et former la communauté universitaire à ces enjeux, et l'accompagner, ainsi que les personnes tierces, dans l'application du cadre normatif institutionnel de la sécurité de l'information.

6.5 Gestionnaire

La, le gestionnaire joue un rôle essentiel dans la protection des systèmes d'information de l'Université. Ses responsabilités à l'égard de la sécurité des systèmes d'information sont, entre autres, de :

a) veiller à ce que les personnes employées et autres personnes dont elle, il est responsable respectent le cadre normatif institutionnel de la sécurité de l'information;

b) coopérer avec la, le CSIO pour mettre en œuvre les mesures de sécurité requises par le cadre normatif institutionnel de la sécurité de l'information;

c) signaler à la personne exploitant un ou des systèmes d'information tout changement de poste, arrêt de travail, cessation d'emploi, de contrat ou de mandat des personnes dont elle, il est responsable afin que les droits d'accès soient revus;

d) rapporter tout incident de sécurité ou activité suspecte en matière de sécurité des systèmes d'information à la, au CSIO, selon le processus établi.

6.6 Responsable d'un système d'information

La, le responsable d'un système d'information s'assure que ce système respecte le cadre normatif institutionnel de la sécurité de l'information ainsi que le cadre de conformité législative et réglementaire. Ses responsabilités incluent notamment le fait de :

a) communiquer à la, au CSIO les informations nécessaires à la classification de sécurité du système d'information;

b) assurer la mise en œuvre des mesures et contrôles requis par le cadre normatif institutionnel de la sécurité de l'information;

c) déterminer les droits d'accès nécessaires en fonction des besoins opérationnels et des principes de sécurité;

d) s'assurer qu'un plan de reprise après sinistre, spécifique au système d'information sous sa responsabilité, est en place et testé régulièrement;

e) rapporter à la, au CSIO tout incident de sécurité ou activité suspecte sur le système d'information.

6.7 Personne exploitant un système d'information

La personne exploitant un système d'information veille à l'application des bonnes pratiques en matière de gestion des accès, de sécurité et de continuité des opérations. Ses responsabilités incluent notamment les éléments suivants :

a) appliquer les contrôles de sécurité définis par le cadre normatif institutionnel de la sécurité de l'information;

b) mettre en œuvre les mesures nécessaires pour protéger les données et les accès;

c) collaborer avec la personne responsable du système d'information pour signaler toute activité suspecte ou incident de sécurité à la, au CSIO;

d) accorder et gérer les droits d'accès en fonction des besoins opérationnels et des principes de sécurité;

e) participer à l'élaboration et aux tests des plans de reprise après sinistre.

6.8 Personne administratrice d'un système d'information

L'administratrice, l'administrateur d'un système d'information est une personne membre du personnel chargée de veiller à la mise en place, à la maintenance et à la sécurisation des systèmes d'information.

Ses responsabilités incluent notamment : la gestion des accès, en collaboration avec la personne exploitant le système d'information, des performances, des mises à jour, des sauvegardes et des mesures de protection afin d'assurer la disponibilité et l'intégrité des systèmes d'information et la confidentialité des données qu'ils contiennent.

6.9 Personne utilisatrice d'un système d'information

La personne utilisatrice d'un système d'information peut être une personne membre de la communauté universitaire ou un tiers qui utilise un système d'information. Ses responsabilités sont, entre autres, de :

a) n'utiliser les systèmes d'information qu'à des fins expressément définies par le cadre normatif institutionnel de la sécurité de l'information;

b) respecter toutes les mesures de sécurité en place en vertu du cadre normatif institutionnel de la sécurité de l'information;

c) respecter la confidentialité des données conservées sur les systèmes;

d) prendre connaissance des communications officielles de l'Université et suivre les consignes spécifiques de sécurité communiquées;

e) informer la, le CSIO, par le processus établi, de toute situation où la sécurité d'un système d'information est jugée vulnérable ou compromise.

7. Gestion de la sécurité des systèmes d’information

7.1 Organisation interne

Afin d'assurer une gestion efficace de la sécurité des systèmes d’information au sein de l’Université, celle-ci doit définir la structure organisationnelle soutenant la planification, le développement, la mise en œuvre et le contrôle des mesures de sécurité afférentes.

7.2 Droits d’accès aux systèmes d’information

7.2.1 Principe de nécessité

Les droits d’accès aux systèmes d’information doivent être octroyés aux personnes à qui ils sont nécessaires afin de remplir leur fonction, de consulter ou d’exploiter des données. Ainsi, les données que les systèmes institutionnels supportent ne doivent être divulguées qu'aux personnes dont les fonctions le nécessitent et conformément aux obligations législatives et réglementaires.

7.2.2 Gestion des identités

La gestion des identités doit être effectuée selon la Directive sur la gestion des identités et des accès. Le cycle de vie des identifiants doit être défini, documenté et communiqué aux personnes concernées.

7.2.3 Gestion des droits d’accès

La gestion des droits d’accès aux systèmes d’information doit être effectuée selon la Directive sur la gestion des identités et des accès.

7.2.4 Contrôle d’accès

Tout système d’information qui conserve des données protégées ou classifiées au sens du Modèle de classification gouvernemental doit disposer d'un mécanisme d'authentification actif contrôlant les accès au système d’information, garantissant ainsi que ces données ne sont pas indûment consultées, divulguées, modifiées, supprimées ou rendues indisponibles.

7.3 Mesures minimales de sécurité

Pour tout système d’information, la, le CSIO doit définir les mesures de sécurité minimales proportionnelles au niveau de classification de sécurité. La personne administratrice d’un système d’information est responsable de leur application.

7.4 Développement, retrait et maintenance

Le développement, le retrait et la maintenance des systèmes d’information doivent être effectués en conformité avec la Directive sur l’administration des systèmes d’information.

Les exigences de sécurité doivent être définies conjointement par la personne responsable du système et la, le CSIO dès la phase d’analyse et validée avant la sélection, la mise en production, l’évolution ou le retrait d’un système d’information.

8. Gestion des incidents

La, le CSIO définit les normes et établit les marches à suivre en matière de gestion des incidents de sécurité informatique afin de garantir une réponse efficace et pertinente, tout en assurant la mise en place d'une équipe capable de les traiter.

Chaque incident doit faire l'objet d'un suivi auprès des parties prenantes pour analyse, évaluation, communication des résultats pertinents et proposition de mesures correctives.

8.1 Mesures d'urgence

Si l'incident requiert une intervention d'urgence pour protéger l'intégrité ou la disponibilité des systèmes d'information, les Services informatiques, de concert avec la, le CSIO, après avoir pris les moyens raisonnables pour aviser les responsables de systèmes d'information et les personnes utilisatrices, peuvent poser les actions appropriées selon le cas, par exemple :

a) interrompre ou révoquer temporairement les services offerts;

b) intervenir sur un système d'information suspecté de contrevenir à la présente politique, aux règlements ou aux lois en vigueur;

c) appliquer les différentes fonctions de diagnostic sur les systèmes d'information;

d) mettre en place les mesures correctives requises afin de circonscrire les impacts.

8.2 Reprise après incident

La, le CSIO définit un plan de reprise après incident visant à réduire l'impact de l'indisponibilité d'un système d'information, et ainsi, à assurer une reprise des opérations dans les meilleurs délais. Les mesures de reprise doivent être vérifiées périodiquement afin de garantir leur efficacité et leur pertinence.

9. Formation et sensibilisation

La, le CSIO doit déployer un programme qui vise à informer, former et sensibiliser la communauté universitaire sur les menaces, les bonnes pratiques et les conséquences d'une violation de la sécurité des systèmes d'information. Ce programme doit être maintenu à jour et faire l'objet d'une révision annuelle afin de tenir compte de l'évolution des menaces, des pratiques et des besoins de la communauté universitaire. L'objectif est de permettre à chaque personne de reconnaître les situations à risque et d'adopter des comportements appropriés et éthiques. Ces formations doivent être accessibles et fortement recommandées à toutes, tous les membres du personnel.

La, le CSIO a la responsabilité de fournir aux personnes utilisatrices d'un système d'information les renseignements nécessaires à la compréhension de leurs obligations en matière de sécurité de l'information.

10. Suivi et contrôle des activités de sécurité de l’information

10.1 Contrôle et vérification

Dans le cadre des activités de contrôle et de vérification, l’Université et ses représentantes, représentants ont l’obligation de respecter la dignité, la liberté d’expression, la liberté de pensée, la liberté académique et la vie privée des membres de la communauté.

Afin de mieux évaluer son exposition aux risques, l’Université doit disposer d'une infrastructure et de processus de journalisation adaptés. L'efficacité des méthodes, processus et mécanismes de protection fait l’objet d’une évaluation continue, et ceux-ci sont ajustés en fonction de l'évolution des menaces et des vulnérabilités.

La, le responsable d’un système d’information, la supérieure immédiate, le supérieur immédiat, la, le CSIO sont autorisés à mandater une représentante, un représentant et à procéder à toutes les vérifications d’usage estimées nécessaires pour s’assurer du respect des dispositions du cadre normatif institutionnel de la sécurité de l’information ainsi que des règles d'utilisation, ententes et protocoles pertinents de l'Université ou des lois et règlements provinciaux ou fédéraux.

Dans le cas d’une vérification qui impliquerait l’accès à des renseignements personnels confidentiels, que ces données soient l’objet ou non de la vérification, toute surveillance ou contrôle abusifs doivent être évités.

Une vérification des renseignements personnels confidentiels d’une personne utilisatrice ou de son utilisation des actifs informationnels ne peut être effectuée sans le consentement de cette personne, à moins que la supérieure immédiate, le supérieur immédiat, la, le responsable d’un système d’information, la, le CSIO n’aient des motifs valables de croire que cette dernière contrevient à l’une ou l’autre des dispositions du cadre normatif institutionnel de la sécurité de l’information.

De plus, cette vérification ne peut être entamée qu’après avoir obtenu l’autorisation de la vice-rectrice, du vice-recteur à la Vie académique dans le cas des personnels enseignants et des personnes étudiantes ou de la vice-rectrice, du vice-recteur au Développement humain et organisationnel dans le cas des personnels non enseignants, et de la vice-rectrice, du vice-recteur aux Systèmes d’information ou, en cas d’absence desdites vice-rectrices, desdits vice-recteurs, de la rectrice, du recteur.

L’utilisation de la technologie pour les activités de contrôle et de vérification ne doit pas permettre de surveiller, sans motif valable, les faits et gestes des personnes utilisatrices ni le contenu de leurs communications.

Cette restriction ne s’applique cependant pas aux activités de journalisation, lesquelles sont nécessaires pour assurer la pérennité des services à la communauté. C’est alors la consultation et l’interprétation de renseignements personnels confidentiels qui ne peuvent être faites sans motif valable, conformément au processus de vérification décrit ci-dessous.

Dans l’éventualité où une vérification des renseignements personnels confidentiels d’une personne utilisatrice ou de son utilisation des actifs informationnels a été effectuée et que l’ensemble du processus de vérification et des activités qui en découlent est complété, celle-ci

doit être informée de la vérification qui a eu lieu et des renseignements qui ont été consultés dans ce cadre.

10.2 Conséquences et sanctions

Le non-respect de la présente politique, du cadre normatif institutionnel de la sécurité de l'information et des mesures de sécurité de l'information qui en découlent peut entraîner le retrait sans préavis des droits d'accès aux systèmes d'information de l'Université pour toute personne utilisatrice, qu'elle soit membre de la communauté universitaire, une sous-traitante, un sous-traitant, une, un prestataire de service, une invitée, un invité ou autre.

Toute contravention à la présente politique, au cadre normatif institutionnel de la sécurité de l'information et aux mesures de sécurité de l'information qui en découlent par une personne physique ou morale agissant comme prestataire de services, sous-traitante, sous-traitant ou invitée, invité de l'Université s'expose aux sanctions ou recours prévus au contrat la, le liant à l'Université et à la législation applicable.

Toute contravention à la présente politique, au cadre normatif institutionnel de la sécurité de l'information et aux mesures de sécurité de l'information qui en découlent par une, un membre du personnel ou de la communauté étudiante l'expose, à la discrétion de l'Université, aux mesures prévues au Règlement nº 2 de régie interne, au Règlement nº 10 sur la protection des personnes et des biens ou aux sanctions et recours prévues par la loi, les règlements, contrats, protocoles ou conventions collectives applicables selon son statut.

Toute personne qui a connaissance de la non-conformité ou du non-respect de cette politique doit en informer sa supérieure immédiate, son supérieur immédiat ou la, le CSIO.

10.2.1 Personnes étudiantes

Les cas impliquant des personnes étudiantes sont référés à la vice-rectrice à la Vie académique, qui assure le suivi requis et prend les actions appropriées, incluant des sanctions, le cas échéant, selon le cadre normatif institutionnel applicable.

Si la situation présente des éléments laissant croire que la sécurité des systèmes d'information de l'Université pourrait être compromise, la, le CSIO peut mettre en place des mesures assurant la sécurité de ces actifs informationnels dans le respect des droits des personnes étudiantes concernées.

10.2.2 Membres du personnel

Les cas impliquant des membres du personnel sont référés à la personne supérieure immédiate ou à la directrice, au directeur du Service du personnel enseignant dans le cas d'une personne enseignante, qui assurent le suivi requis et prennent les actions appropriées, incluant des sanctions, le cas échéant, selon le cadre normatif applicable et selon le statut de la personne impliquée.

Si la situation présente des éléments laissant croire que la sécurité des systèmes d'information de l'Université pourrait être compromise, la, le CSIO peut mettre en place des mesures assurant la sécurité de ces actifs informationnels dans le respect des droits des membres du personnel concernés.

10.2.3 Autres personnes

Les cas impliquant toute personne autre qu'une personne employée ou étudiante sont pris en charge par la, le CSIO.

10.3 Respect de la politique et dérogation aux exigences de sécurité

La présente politique et les directives y étant associées doivent être appliquées en fonction des besoins d'affaires de l'Université. Leur application doit représenter des avantages de sécurité excédant les inconvénients qu'ils impliquent, s'il en est.

Compte tenu de ce qui précède, il est possible que, pour la réalisation des missions de l'Université, des situations spécifiques rendent difficile le respect de certaines exigences en matière de sécurité des systèmes d'information. Dans un tel contexte, une demande de dérogation aux exigences de sécurité est nécessaire pour s'assurer qu'elle soit correctement analysée, approuvée et suivie.

10.3.1 Demande de dérogation aux exigences de sécurité

La demande de dérogation doit être soumise selon le processus prévu à la, au CSIO, qui est responsable de l'étudier et de coordonner une consultation auprès des personnes intervenantes concernées (personne requérante, protectrice, protecteur universitaire, Vice-rectorat à la vie académique dans le cas des personnes enseignantes, ou Vice-rectorat au développement humain et organisationnel dans le cas des personnes non enseignantes).

10.3.2 Décision au sujet d'une demande de dérogation aux exigences de sécurité

L'étude des demandes de dérogation aux exigences de sécurité prévues par la présente politique et ses directives associées est de la responsabilité de la, du CSIO. Une décision est rendue à la suite de son étude du dossier et de la consultation des personnes intervenantes concernées.

Cette décision est rendue par écrit, motivée et dans un délai raisonnable à compter de la réception de la demande. Lorsque la décision approuve la dérogation, elle doit en préciser la portée et la durée, ainsi que toutes les modalités qui y sont associées.

Dans le cas où la personne requérante est en désaccord avec la décision rendue par la, le CSIO, elle peut présenter par écrit une demande de révision de la décision auprès de la vice-rectrice, du vice-recteur aux Systèmes d'information, qui pourra, si elle, il le juge approprié, consulter les personnes intervenantes concernées et émettre une décision finale quant à la demande de dérogation.

11. Responsable de l'application

La vice-rectrice, le vice-recteur aux Systèmes d'information est responsable de l'application de cette politique.

12. Entrée en vigueur

La présente politique entre en vigueur au moment de son adoption par le Conseil d’administration.

13. Mise à jour

La présente politique est mise à jour minimalement tous les trois ans.

Tableau historique des modifications

Historique des modifications		
Résolution	Date d'adoption	Articles modifiés
2026-A-19920	18 juin 2026	Nouveau gabarit[1] et refonte complète

[1] À cette date, en respect de la Directive sur l'élaboration, l'approbation et la diffusion des règlements, politiques, directives et procédures, ce document normatif a fait l'objet d'une modification quant à sa forme pouvant avoir eu un impact sur la numérotation des articles.