N° IST-05

Titre :	**Politique de gestion des incidents liés à la sécurité de l'information**
CLASSIFICATION	TECHNOLOGIES & SYSTÈMES D'INFORMATION
PREMIÈRE ADOPTION :	26 septembre 2017
MODIFIÉE LE :	15 janvier 2026

Cette politique a été adoptée en anglais. En cas de divergence la version anglaise prévaut sur la version française.

1 Objectif

La présente politique a pour objectif d'établir une approche structurée et efficace pour gérer les incidents liés à la sécurité de l'information qui pourraient avoir une incidence sur la confidentialité, l'intégrité et la disponibilité des actifs informationnels du Collège Dawson.

Cette politique s'inscrit dans le cadre de la stratégie de sécurité de l'information du Collège Dawson et est conforme à la politique-cadre sur la sécurité de l'information (n° BOG-DG-01) et à la politique de sécurité informatique (n° IST-01).

2 Contexte juridique

Chapitre G-1.03 - *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI), Gouvernement du Québec, 1er janvier 2025*

Processus GMVI - *Processus de gestion des menaces, des vulnérabilités et des incidents (GMVI), Ministère de la Cybersécurité et du Numérique (MCN), 2022*

N° BOG-DG-01, *Politique-cadre sur la sécurité de l'information, Collège Dawson, 2018*

3 Champ d'application

Cette politique s'applique à :

- Tous les employés, étudiants, sous-traitants et parties prenantes du Collège Dawson qui utilisent ou gèrent les systèmes d'information, les réseaux et les données du Collège.
- Tous les actifs numériques (tels que les appareils, les réseaux, les systèmes, les applications, les données) et les services gérés ou exploités par le Collège.
- Tous les incidents susceptibles d'affecter les actifs numériques.

4 Énoncé de politique

Le Collège Dawson s'engage à :

- Assurer la détection, le signalement, la réponse et la reprise rapides en cas d'incidents liés à la sécurité de l'information.
- Minimiser l'impact des incidents sur les opérations et la réputation.
- De respecter toutes les obligations légales, réglementaires et contractuelles liées à la réponse aux incidents.
- Améliorer continuellement le processus de gestion des incidents.

5 Définitions

5.1 Plan de continuité des activités

Plan détaillé décrivant comment l'organisation poursuivra ses activités pendant et après une crise.

5.2 Plan de reprise après sinistre

Plan formel et documenté visant à restaurer les systèmes et fonctions informatiques critiques de l'organisation après une perturbation majeure.

5.3 Événement lié à la sécurité de l'information

Événement indiquant une possible violation de la sécurité de l'information ou une défaillance des contrôles[1] .

[1] ISO/IEC 27035-1:2023, 3.1.4

5.4 Incident de sécurité de l'information

Événement(s) de sécurité de l'information connexe(s) et identifié(s) pouvant nuire aux actifs d'une organisation ou compromettre ses opérations[2] , tel que les violations de données, les accès non autorisés, les infections par des logiciels malveillants, les attaques par déni de service ou les incidents ayant une incidence sur la disponibilité des systèmes d'information.

6 Rôles et responsabilités

6.1 Direction générale

- Active le comité de gestion de crise si la situation créée par l'incident menace la mission, les objectifs stratégiques ou la réputation du Collège.
- Préside le comité de gestion de crise

6.2 Comité de gestion de crise

- Comprend le comité de direction
- Coordonne et veille à l'application des plans de continuité des activités des unités
- Dirige les efforts d'intervention pendant les situations de crise découlant de l'incident

6.3 Responsable des incidents

- Attribué au directeur ou directrice des technologies et systèmes d’information ou à son délégué
- Conseille la direction générale sur l'activation du plan de reprise informatique
- Agit en tant que responsable informatique au sein du comité de gestion de crise
- Supervise la capacité de gestion des incidents de l'organisation.
- Examine et approuve la présente politique

6.4 Coordonnateur ou coordinatrice initial des incidents

- Attribué au gestionnaire du support informatique ou à son délégué
- Dirige les activités de réponse aux incidents et coordonne l'équipe de réponse aux incidents
- Évalue l'incident
- Forme et dirige une équipe ad hoc de réponse aux incidents
- Signale les incidents majeurs au coordinateur ou coordinatrice des incidents
- Documente toutes les activités et mesures prises en rapport aux incidents

[2] ISO/IEC 27035-1:2023, 3.1.5

6.5 Coordonnateur ou coordonnatrice des incidents

- Attribué aux personnes ayant le rôle de *COMSI* (*Coordonnateur organisationnel des mesures de sécurité de l'information)*, défini par le MCN comme le coordonnateur opérationnel des mesures de sécurité.
- Forme et dirige une équipe ad hoc d'intervention en cas d'incident
- Est responsable de la direction de toutes les activités d'intervention en cas d'incident majeur et de la coordination de l'équipe d'intervention en cas d'incident
- Veille à ce que les informations appropriées soient communiquées en temps utile au responsable des incidents.
- Si un incident se prolonge au-delà d'un quart de travail et nécessite la présence d'une personne, un autre coordinateur ou coordinatrice des incidents doit prendre la relève avec toutes les informations et l'autorité nécessaires

6.6 Équipes d'intervention en cas d'incident

- Composition ad hoc selon la nature de l'incident, comprenant le coordonnateur ou coordinatrice des incidents et divers rôles supervisant les opérations de sécurité.
- Traite l'incident ou une partie de l'incident
- Exécute le processus d'intervention en cas d'incident, coordonne le confinement et la reprise.

7 Processus de gestion des incidents

Le processus de gestion des incidents liés à la sécurité de l'information comprend cinq phases distinctes :

1. planifier et préparer
2. détection et signalement
3. évaluer et décider (catégoriser et hiérarchiser)
4. réagir et rétablir la situation
5. Activités post-incident : tirer des leçons, apporter des améliorations

8 Coordination, escalade et rapport

Une fois un incident signalé, une évaluation préliminaire est effectuée et un dossier est ouvert dans le système de gestion des incidents. En fonction de la complexité, de la gravité, de l'impact et de l'urgence, un billet d'incident sera attribué, réattribué ou escaladé.

Si l'incident constitue une situation de crise, la coordination sera escaladée au comité de crise du Collège par l'intermédiaire du responsable des incidents. Le comité de crise gérera la réponse à la situation de crise.

Outre la portée et la gravité de l'incident, l'évaluation de l'incident permet de déterminer s'il y a des renseignements personnels en jeu et s'il relève du gouvernement.

Les incidents impliquant des renseignements personnels sont signalés au directeur ou directrice des affaires corporatives, qui peut également les signaler à la *Commission d'accès à l'information*.

Si l'incident relève du gouvernement, il doit être signalé à celui-ci conformément au processus GMVI par le coordonnateur des incidents.

9 Communication et notification

En cas d'incident de sécurité, le Collège Dawson s'engage à faire preuve de transparence tout au long du processus. Le canal de communication sera choisi parmi les options suivantes, en fonction des circonstances et des technologies disponibles.

- Courriel
- Système d'interphone
- Téléphone cellulaire
- Omnivox
- Site web
- Médias
- Autres

10 Formation et sensibilisation

Tout le personnel impliqué dans les activités de gestion des incidents recevra une formation continue afin d'identifier les incidents de sécurité et d'y répondre. Des exercices de simulation périodiques seront organisés afin d'évaluer leur état de préparation.

11 Révision et maintenance

La présente politique sera révisée chaque année ou après tout incident majeur afin de s'assurer qu'elle reflète la structure organisationnelle, les processus et les technologies les plus récentes susceptibles d'avoir une incidence sur la gestion des incidents.