CHAMPLAIN
REGIONAL COLLEGE

Directive relative au signalement des incidents liés à la sécurité de l'information et à la protection contre les cybermenaces

Champlain COLLEGE LENNOXVILLE
1958
St.Lawrence CEGEP CHAMPLAIN
Champlain COLLEGE SAINT-LAMBERT

Historique des révisions

Version	Date	Par	Type	Commentaires
0.1	23 août 2024	Claude Leduc	Création	
0.2	26 septembre 2024	Claude Leduc	Modification	Relecture du texte
0.3	30 septembre 2024	Claude Leduc	Modification	Ajout de précisions suite à des commentaires internes
0.4	6 novembre 2024	Claude Leduc	Modification	Révision du texte suite à l'examen par le directeur général
1.0	8 novembre 2024	Claude Leduc	Autorisation	Autorisé par le directeur général

Table des matières

1. Préambule

La présente directive sur le signalement des incidents liés à la sécurité de l'information et à la protection contre les cybermenaces (ci-après la « directive ») fait partie du cadre de gestion de la sécurité de l'information.

Le Collège régional de Champlain (le « Collège ») met en œuvre la présente directive afin de promouvoir certains réflexes chez ses employés et de les guider en cas d'incident de sécurité de l'information, y compris en ce qui concerne les mesures préventives contre les cybermenaces.

2. Objectif

La directive a pour objet d'informer toutes les personnes et entités, qu'elles soient régulières, occasionnelles ou contractuelles, quel que soit leur statut, qui utilisent les actifs informationnels du Collège, des mesures à prendre en cas d'incident de sécurité de l'information.

Elle précise également les mesures à prendre pour contrer les cybermenaces.

3. Cadre juridique et réglementaire

La directive s'appuie sur les lois, règlements et normes suivants :

- La directive gouvernementale sur la sécurité de l'information
- Le cadre gouvernemental de gestion de la sécurité de l'information
- Loi concernant le cadre juridique des technologies de l'information (LRQ, c. C-1.1)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, c. A-2.1)
- Règlement sur les incidents de confidentialité (LRQ, c. A-2.1, r. 3.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, c. G-1.03)
- 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 (LRQ, c. G-1.03, r. 1)
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (LRQ, c. A-2.1, r 2)
- Cadre de gestion des risques et des incidents à portée gouvernementale
- Pratiques gouvernementales en matière de sécurité de l'information
- Exigences du *ministère de la Cybersécurité et du Numérique* et des *Centres opérationnels de cyberdéfense (COCD)*
- Tous les règlements, politiques et règlements du Collège

4. Champ d'application

Dans le cadre de la politique de sécurité de l'information du Collège et de son cadre de gestion de la sécurité de l'information connexe, la présente directive s'applique à toutes les personnes et entités du Collège, qu'elles soient permanentes, occasionnelles ou contractuelles, quel que soit leur statut, qui utilisent les ressources informationnelles du Collège.

5. Définitions

Actif informationnel : Toute information numérique, tout document numérique, tout système d'information, toute documentation, tout équipement informatique, toute technologie de l'information, toute installation ou tout ensemble de ces éléments acquis ou créés par le Collège pour mener à bien sa mission.

Le **Collège :** désigne le Collège régional Champlain dans son ensemble, qui offre des programmes d'enseignement général et professionnel, ainsi que ses collèges constituants.

COMSI : coordonnateur organisationnel des mesures en sécurité de l'information. Les COMSIs participent à la mise en œuvre des mesures et fournissent le soutien nécessaire au chef de la sécurité de l'information organisationnelle (CSIO), notamment en ce qui concerne la gestion des incidents et des risques liés à la sécurité de l'information.

CSIO : chef de la sécurité de l'information organisationnelle. Le CSIO est responsable de la gestion globale de la sécurité de l'information au sein du Collège. Il travaille en étroite collaboration avec les parties prenantes gouvernementales concernées par la sécurité de l'information afin de garantir le respect des exigences en la matière.

Cybermenace : événement perçu, crédible, potentiel et appréhendé, avec une probabilité non nulle, susceptible de compromettre la sécurité de l'information.

Incident : événement affectant ou pouvant affecter la disponibilité, l'intégrité ou la confidentialité des informations, ou plus généralement la sécurité des systèmes d'information, comme une interruption ou une dégradation des services.

Gestionnaire : Autorité administrative au sein d'un département ou d'une unité, qu'elle soit pédagogique ou administrative.

6. Que faire en cas d'incident lié à la sécurité de l'information

En cas d'incident lié à la sécurité de l'information, veuillez suivre les directives suivantes :

- **Signalez l'incident :** contactez immédiatement votre service informatique local ;
- **Recueillez des informations :** si possible, recueillez toutes les informations pertinentes, telles que la date, l'heure, les circonstances et les messages d'erreur afin de documenter l'incident ;
- **Ne supprimez pas les données :** évitez de supprimer des éléments qui pourraient servir de preuves ou être utiles pour une analyse ultérieure ;
- **Confidentialité :** ne communiquez l'incident qu'aux personnes qui ont besoin de le connaître pour le résoudre ;
- **Ne payez pas de rançon :** si l'on vous demande de le faire, ne le faites pas et contactez immédiatement votre service informatique local ;
- **N'éteignez pas votre poste de travail :** il est important de ne pas éteindre votre poste de travail, car cela pourrait entraîner la perte de preuves utilisées lors de l'analyse ;
- **Suivez les recommandations informatiques :** respectez toutes les consignes fournies par le personnel informatique pour assurer une gestion efficace des incidents.

7. Prévention des cybermenaces

Pour lutter contre les cybermenaces, prenez les mesures suivantes :

- Ne téléchargez pas de logiciels ou d'utilitaires non autorisés. En cas de doute, contactez votre service informatique local ;
- Ne connectez pas de périphérique de stockage USB ou de support amovible d'origine inconnue à un appareil du collège ;
- Ne cliquez pas sur des liens hypertextes provenant de sources inconnues, n'ouvrez pas de pièces jointes suspectes et ne scannez pas de codes QR ;
- Si vous recevez un courriel malveillant (ou qui semble potentiellement malveillant) contenant un virus ou une autre alerte :
    - Ne faites pas ce qui suit :
        - prendre aucune mesure ;
        - répondre ;
        - suivre les instructions contenues dans le courriel.
    - Informez votre service informatique local et transférez-lui le courriel si nécessaire.

8. Rôles et responsabilités

Pour que les mesures de sécurité de l'information soient efficaces, il est essentiel que les rôles et responsabilités de chaque partie prenante au sein du Collège soient clairement définis.

8.1. Le directeur général

- Approuve la présente directive ;
- Veille à ce que des activités de formation et de sensibilisation des employés soient menées.

8.2. Directeur du collège constituant

Il ou elle agit en tant qu'autorité du collège constituant en matière de sécurité de l'information, conformément à l'autorité qui lui a été déléguée par le directeur général. Le directeur du collège constituant veille pour sa part au respect et à l'application de la présente directive au sein de son collège.

8.3. Chef organisationnel de la sécurité de l'information (CSIO)

- Élabore et veille à la mise en œuvre et à la révision de la présente directive ;
- Veille à ce que des activités de sensibilisation et de formation soient menées pour soutenir la mise en œuvre de la directive.

8.4. Coordonnateur organisationnel des mesures en sécurité de l'information (COMSI)

- Met en œuvre la présente directive ;
- Mène des activités de sensibilisation et de formation pour soutenir la mise en œuvre de la directive ;
- Applique les mesures d'intervention appropriées à toute menace ou incident lié à la sécurité de l'information afin de garantir la sécurité des informations ciblées.

8.5. Services des technologies de l'information

- Responsables de l'application de la présente directive sur leur site ;
- Signale immédiatement tout incident lié à la sécurité de l'information aux COMSIs et/ou au CSIO du Collège ;
- Collabore activement avec les COMSIs pour répondre à tout incident ou menace de sécurité informatique signalé ou détecté.

8.6. Gestionnaires

- Veillent à la mise en œuvre et à l'application des mesures de sécurité de l'information, y compris de la présente directive, au sein de leur département ou service ;
- Signalent tout événement ou toute menace liée à la sécurité de l'information à leurs services informatiques locaux ;
- Veillent à ce que la présente directive soit communiquée à tous les employés, partenaires et sous-traitants de leur département et/ou service, ou associés à ceux-ci.

8.7. Personnel du Collège et étudiants

- Informer immédiatement les services informatiques locaux de tout incident lié à la sécurité de l'information dont ils ont connaissance (piratage, intrusion dans un système informatique, usurpation d'identité, utilisation de virus informatiques, etc.) ;
- Participer à toute action entreprise pour identifier ou atténuer une menace ou un incident lié à la sécurité de l'information ;
- Se conformer aux mesures préventives contre les cybermenaces.

9. Diffusion et mise à jour de la présente directive

Le chef organisationnel de la sécurité de l'information (CSIO) est responsable de la mise à jour de la présente directive.

Le Comité de la haute direction (SMC), en collaboration avec le CSIO, est responsable de la diffusion de la présente directive.

La présente directive fera l'objet d'une évaluation et d'une révision régulières, notamment en ce qui concerne la pertinence de ses dispositions par rapport aux nouveaux enjeux en matière de sécurité de l'information.

10. Date d'entrée en vigueur

La présente directive entre en vigueur à la date de son approbation par le directeur général et reste en vigueur jusqu'à ce qu'elle soit abrogée, modifiée ou remplacée par une autre directive.