Politique de Sécurité de l'Information

Mise en place pour le "Collège Cumberland"

Raphael Nga Beauregard

François-Xavier Leclerc

Sanders Bernavil

Robin Boucher

Présenté à

Mohamed Rida Allah

CYF AM - Gestion de risques

Janvier 2025

Collège Cumberland

Montreal, QC

1. (Raph) La politique de sécurité du Collège Cumberland a pour objectif principal de protéger les informations et les systèmes de l'établissement contre les menaces internes et externes, afin d'assurer la confidentialité, l'intégrité et la disponibilité des ressources informationnelles. Cette politique vise également à sensibiliser le personnel, les étudiants et les autres utilisateurs aux risques liés à la sécurité de l'information et à définir les responsabilités de chacun en matière de protection des données. Elle s'applique à l'ensemble des employés, des étudiants, des consultants, des fournisseurs et de toute autre personne ayant accès aux systèmes d'information du Collège Cumberland, qu'ils soient situés sur le campus ou à l'extérieur. Elle couvre tous les aspects de la sécurité de l'information, y compris les données, les logiciels, le matériel informatique, les réseaux, les communications et les locaux.

2. Le Collège Cumberland joue un rôle crucial dans la formation des futurs professionnels et citoyens. En tant que tel, il collecte, stocke et traite une grande quantité d'informations sensibles, notamment des données personnelles sur les étudiants (nom, adresse, date de naissance, notes, dossier scolaire, etc.), les employés (informations personnelles, salariales, médicales, etc.) et les anciens élèves, ainsi que des informations financières (données relatives aux finances du collège, y compris les budgets, les états financiers, les informations sur les donateurs), académiques (curriculum, plans de cours, matériel pédagogique, résultats de recherche) et administratives (procédures internes, documents stratégiques, contrats). Ces données sont stockées et traitées dans divers systèmes d'information critiques, tels que les systèmes de gestion des étudiants (SGE), les systèmes de gestion des ressources humaines (GRH), les systèmes financiers, les systèmes de gestion de l'apprentissage (SGA) et le réseau informatique.

Cependant, le Collège Cumberland est confronté à un environnement de menaces complexe et en constante évolution. Les cyberattaques, telles que les logiciels malveillants (virus, vers, chevaux de Troie, ransomwares), le phishing (tentatives d'hameçonnage), les attaques par déni de service (DoS) et les intrusions (accès non autorisé, vol de données, sabotage), représentent une menace majeure. Les menaces

internes, telles que les erreurs humaines (suppression accidentelle de fichiers, envoi de courriels à de mauvais destinataires), la négligence (manque de vigilance dans l'application des mesures de sécurité, utilisation de mots de passe faibles) et les accès non autorisés, constituent également un risque important. De plus, les catastrophes naturelles (incendies, inondations, tremblements de terre) peuvent endommager ou détruire les équipements informatiques et les données, tandis que les risques liés aux tiers (vulnérabilités chez les fournisseurs, partenaires) peuvent être exploités pour accéder aux systèmes du collège ou voler des données. Il est donc essentiel de mettre en place une politique de sécurité robuste et adaptée pour protéger ces informations et assurer la continuité des activités du Collège Cumberland.

3.(SBC)

3. Rôles et responsabilités

3.1 Direction du Collège

La direction est responsable de la mise en place et du suivi de la politique de sécurité de l'information. Ses responsabilités incluent :

- Définir les orientations stratégiques en matière de sécurité de l'information.
- Assurer la conformité aux lois et réglementations applicables.
- Allouer les ressources nécessaires à la mise en œuvre des mesures de sécurité.
- Établir un comité de sécurité de l'information.

3.2 Gestionnaires et responsables de départements

Les gestionnaires et responsables de départements doivent :

- Appliquer et faire respecter la politique de sécurité de l'information au sein de leurs équipes.

- Assurer la sensibilisation et la formation des employés sur les bonnes pratiques de sécurité.
- Signaler tout incident de sécurité à l'équipe responsable.
- Collaborer avec l'équipe de sécurité pour la mise en œuvre des mesures de protection des données.

3.3 Employés et membres du personnel

Tous les employés et membres du personnel ont un rôle clé dans la protection des informations du collège. Ils doivent :

- Respecter les directives et procédures de sécurité de l'information.
- Utiliser les ressources informatiques de manière responsable et sécurisée.
- Signaler toute tentative d’accès non autorisé ou tout incident de sécurité.
- Suivre les formations en sécurité mises en place par l’établissement.

3.4 Équipe de sécurité informatique

L’équipe de sécurité informatique est chargée de la gestion opérationnelle de la sécurité de l’information. Elle doit :

- Développer et mettre à jour les procédures de sécurité.
- Surveiller et analyser les menaces et les vulnérabilités.
- Réagir aux incidents de sécurité et mettre en place des mesures correctives.
- Assurer la protection des systèmes et des réseaux contre les cyberattaques.

3.5 Étudiants

Les étudiants, bien que n’étant pas directement responsables de la sécurité institutionnelle, doivent :

- Respecter les règles d’utilisation des ressources informatiques du collège.

- Protéger leurs identifiants et mots de passe.
- Signaler toute activité suspecte aux autorités compétentes.

4.(SBC)

4. Politique de sécurité

4.1 Objectifs

- Assurer la confidentialité, l'intégrité et la disponibilité des informations.
- Protéger les données personnelles et institutionnelles contre tout accès non autorisé.
- Prévenir et gérer les incidents de sécurité de l'information.
- Sensibiliser et former l'ensemble du personnel aux bonnes pratiques en matière de sécurité.

4.2Contrôles de sécurité

Pour protéger les actifs informationnels, plusieurs contrôles de sécurité seront mis en place :

- **Contrôles d’accès** : Mise en place d’authentifications fortes (MFA), gestion des droits et permissions selon les besoins.
- **Protection des infrastructures** : Sécurisation des serveurs, pare-feu, antivirus, mises à jour régulières.
- **Chiffrement des données** : Utilisation de protocoles sécurisés pour le stockage et la transmission des informations sensibles.
- **Surveillance et détection** : Mise en place de systèmes de détection et de prévention des intrusions.

- **Sauvegarde et récupération** : Plan de sauvegarde périodique et procédures de restauration des données en cas d'incident.
- **Sensibilisation et audit** : Contrôles réguliers pour identifier les vulnérabilités et renforcer la formation des utilisateurs.

5. (FX)

Gestion des incidents

Le Collège Cumberland devrait établir des procédures claires pour assurer une gestion efficace des incidents de sécurité de l'information. Une approche bien définie permettrait de limiter les dommages, d'identifier les causes et de prévenir la récurrence des incidents.

5.1 Procédures de signalement des incidents

Le Collège devrait mettre en place un processus structuré pour signaler rapidement les incidents de sécurité. Tous les employés, y compris le personnel administratif et enseignant, devraient être informés des canaux appropriés pour signaler une menace ou une violation de sécurité.

1. **Mécanismes de signalement**
    - Une adresse courriel dédiée et un formulaire en ligne sécurisé devraient être mis à disposition pour signaler les incidents.
    - Une ligne téléphonique de support devrait être accessible 24/7 pour les urgences de cybersécurité.
    - Un protocole interne devrait être défini pour assurer un signalement rapide aux responsables de la sécurité de l'information.

2. **Formation et sensibilisation**
    - Les employés devraient recevoir une formation régulière sur la manière d'identifier et de signaler les incidents.
    - Des rappels périodiques sous forme de bulletins internes et d'affiches informatives devraient être diffusés pour garantir une vigilance continue.

5.2 Plan de réponse aux incidents

Le Collège devrait disposer d'un plan détaillé de réponse aux incidents afin d'atténuer les impacts et de restaurer la normalité aussi rapidement que possible. Ce plan devrait inclure les étapes suivantes :

1. **Identification et évaluation**
    - Une équipe dédiée à la gestion des incidents devrait être mise en place pour évaluer chaque menace signalée.
    - Des outils de surveillance automatisés devraient être utilisés pour détecter rapidement les anomalies et les activités suspectes.
2. **Confinement et atténuation**
    - Des mesures immédiates devraient être prises pour limiter la propagation de l'incident.
    - Des accès spécifiques pourraient être temporairement restreints pour protéger les données sensibles.
3. **Eradication et récupération**
    - Les équipes techniques devraient supprimer la menace et restaurer les systèmes affectés à partir de sauvegardes sécurisées.
    - Des analyses post-incident devraient être effectuées pour s'assurer que la menace est entièrement éliminée.
4. **Communication et reporting**

- Un protocole de communication interne devrait être défini pour informer les employés concernés.
- Un rapport détaillé de chaque incident devrait être conservé pour une analyse future et une amélioration continue des protocoles de sécurité.

5. **Amélioration continue**
    - Après chaque incident, une rencontre devrait être organisée pour identifier les points d'amélioration.
    - Les politiques et procédures devraient être mises à jour en fonction des leçons apprises afin de renforcer la posture de cybersécurité du Collège.

En adoptant ces mesures, le Collège Cumberland améliorerait sa capacité à gérer efficacement les incidents de sécurité et à protéger ses ressources informationnelles contre les menaces potentielles.

6. (FX)

Sensibilisation et formation

La sensibilisation et la formation en matière de sécurité de l'information devraient être des priorités essentielles pour instaurer une culture de sécurité robuste au sein du Collège Cumberland. En tant qu'établissement offrant des programmes en marketing et en cybersécurité, il serait impératif que tous les employés, y compris le personnel enseignant et administratif, soient bien informés des meilleures pratiques en matière de sécurité et des menaces potentielles.

6.1 Programmes de formation à la sécurité

Le Collège Cumberland devrait mettre en place des programmes de formation structurés et continus pour garantir que chaque employé possède les connaissances et compétences nécessaires pour protéger les actifs informationnels de l'établissement. Ces programmes devraient inclure :

1. **Sessions d'orientation pour les nouveaux employés**

   Dès leur intégration, les nouveaux employés devraient participer à des sessions d'orientation axées sur la sécurité de l'information. Ces sessions devraient couvrir les politiques de sécurité du Collège, les protocoles à suivre en cas d'incident, et les ressources disponibles.

2. **Ateliers pratiques et interactifs**

   Des ateliers réguliers devraient permettre aux employés d'acquérir des compétences pratiques en matière de sécurité. Ces sessions pourraient inclure des simulations d'attaques par hameçonnage ou des exercices de réponse à des incidents.

3. **Modules de formation en ligne**

   Pour offrir une flexibilité maximale, le Collège devrait proposer des modules de formation en ligne couvrant divers sujets, tels que la protection des données personnelles et la sécurité des réseaux. Ces modules devraient être régulièrement mis à jour pour refléter les évolutions des menaces et des technologies.

4. **Formations spécialisées pour le personnel IT**

   Le personnel informatique et les responsables de la sécurité devraient recevoir des formations avancées sur des sujets tels que la gestion des incidents, les tests d'intrusion et la protection des infrastructures critiques.

6.2 Campagnes de sensibilisation

Le Collège Cumberland devrait promouvoir une culture de sécurité proactive grâce à diverses initiatives de sensibilisation :

1. **Journées dédiées à la sécurité**

   Le Collège devrait organiser des événements annuels centrés sur la sécurité de l'information, avec des conférences et des démonstrations pratiques.

2. **Bulletins d'information réguliers**

   Le Collège devrait diffuser des bulletins électroniques contenant des mises à jour sur les menaces émergentes et des conseils pratiques pour renforcer la sécurité personnelle.

3. **Affiches et rappels visuels**

   Des affiches informatives devraient être placées dans les espaces communs pour rappeler les meilleures pratiques en matière de sécurité.

4. **Programme d'ambassadeurs de la sécurité**

   Certains employés pourraient être désignés comme ambassadeurs de la sécurité afin d'animer des ateliers et de promouvoir activement les initiatives de sécurité au sein du Collège.

5. **Tests et audits de sensibilisation**

   Le Collège devrait réaliser périodiquement des tests de sensibilisation, comme des simulations de phishing, pour évaluer la vigilance des employés et adapter les formations en conséquence.

En mettant en place ces mesures, le Collège Cumberland renforcerait sa posture de sécurité et garantirait que ses employés sont bien préparés à faire face aux menaces actuelles et futures.

7. (robin)

Surveillance et révision de la politique de sécurité

La politique de sécurité informatique du Collège Cumberland repose sur une approche proactive, garantissant ainsi la conformité continue, l'adaptation aux nouvelles menaces et aux évolutions technologiques.

Surveillance de la conformité

La surveillance de la conformité est assurée par des contrôles continus et des audits réguliers pour garantir le respect des normes internes et externes en matière de sécurité.

1. **Vérifications régulières** :
    - Des audits internes sont réalisés chaque trimestre pour évaluer l'efficacité des mesures de sécurité.
    - Les vérifications comprennent des scans de vulnérabilité, analyses des journaux d'événements (logs), évaluation de la gestion des identités et des accès, évaluer la formation des employés et une évaluation de la conformité aux normes de sécurité.
    - Les résultats de ces audits sont mis dans des rapports et partagés avec la Direction ainsi que le comité de gouvernance des ressources informationnelles pour une évaluation approfondie.
2. **Enquêtes ciblées** :
    - Des enquêtes sont menées en réponse à des activités suspectes ou à des non-conformités identifiées durant les audits ou dans le cadre des contrôles réguliers.
3. **Indicateurs de performance de la conformité (KPI)** :
    - Des indicateurs clés sont utilisés pour évaluer la conformité des systèmes aux exigences de la politique de sécurité, tels que :
        - Le taux de conformité des systèmes.
        - Le nombre d'incidents de sécurité détectés et résolus.
        - Le temps moyen de réponse aux incidents.
        - Le taux de conformité des audits.
4. **Rétroaction et ajustements** :
    - Après chaque audit ou enquête, des actions correctives et préventives sont recommandées pour résoudre les non-conformités identifiées.
    - Un suivi est réalisé pour assurer que ces actions sont correctement mises en œuvre et respectées dans les délais.

Mise à jour de la politique

1. **Fréquence de mise à jour** :
    - La politique de sécurité est révisée à chaque année, bien que des mises à jour plus fréquentes puissent être nécessaires en réponse à des modifications législatives, des avancées technologiques ou des incidents de sécurité significatifs.
    - Les révisions peuvent aussi être motivées par les résultats des vérifications régulières (chaque 3 mois) ou à la suite d'incidents.
2. **Processus de mise à jour** :
    - Un comité de révision évalue les besoins de mise à jour en fonction des évolutions des risques, des nouvelles normes et des meilleures pratiques.
    - Une fois révisée, la politique est soumise à l'approbation de la Direction avant d'être communiquée à l'ensemble des parties prenantes.
3. **Communication des mises à jour** :
    - La politique est ensuite communiquée à tous les membres de la communauté (étudiants, enseignants, personnel administratif, invités) par des courriels, des réunions d'information ou des sessions de formation.
    - Les mises à jour sont également publiées sur le site Intranet pour une consultation continue.
4. **Gestion des écarts de conformité** :
    - En cas de non-respect de la politique, des actions correctives sont mises en place pour ramener l'organisation en conformité. Cela peut inclure des rappels de la politique, des formations supplémentaires ou des actions disciplinaires dans les cas graves.
    - Un suivi est effectué pour garantir que les mesures correctives sont appliquées efficacement et dans les délais prévus.