CATÉGORIE	Technologie de l'information	**CODE DE SERVICE**	06
Nº DE DOCUMENT	002	**TYPE DE DOCUMENT**	Politique
DESCRIPTION	Cybersécurité		
DATE D'APPROBATION	Décembre 2025	**PROCHAIN EXAMEN**	Décembre 2028
EMPLACEMENT	*IT-06-PL-Cyber Security-002.docx*		

1. Objectif

À la School Boards' Co-operative Inc. (SBCI), la protection des données des conseils scolaires et la sécurité de nos systèmes sont des responsabilités fondamentales. La présente politique en matière de cybersécurité établit les principes et les engagements qui orientent nos efforts visant à assurer la confidentialité, l'intégrité et la disponibilité de l'ensemble des ressources d'information qui nous est confié.

La SBCI est déterminée à considérer la cybersécurité comme une priorité absolue sur le plan opérationnel en assurant ses membres, ses partenaires et les parties intéressées qu'elle gère leurs renseignements selon les paramètres de diligence et de sécurité les plus rigoureux.

2. Portée

La politique vise l'ensemble des systèmes, réseaux, applications et données numériques détenus, exploités ou gérés par la SBCI. Elle s'applique également à tous les employés, entrepreneurs, fournisseurs et tiers ayant accès à nos ressources numériques.

3. Principes directeurs

a. Reddition de comptes et leadership

Pour la SBCI, la cybersécurité constitue une responsabilité fondamentale de l'organisation, qui requiert une surveillance et un leadership actifs. La haute direction fournit une orientation stratégique, affecte des ressources et supervise la mise en œuvre de notre cadre de sécurité. Les rôles et responsabilités en matière de cybersécurité sont bien définis à l'échelle de l'organisation, la reddition de comptes étant ainsi assurée à tous les niveaux. Nous favorisons une culture dans laquelle chaque membre du personnel comprend le rôle qu'il joue dans la protection des systèmes numériques et de l'information qui nous est confiée.

b. Gestion des risques

Notre approche en matière de cybersécurité est fondée sur le risque, et nous reconnaissons que les menaces n'entraînent pas toutes les mêmes répercussions. Les risques font l'objet d'une évaluation sur une base régulière afin de cerner les menaces potentielles, les vulnérabilités et leurs conséquences éventuelles sur nos activités et nos membres, ce qui nous permet d'accorder la priorité aux investissements en sécurité et de mettre en œuvre des mesures de protection là où les besoins sont les plus criants. Les décisions qui concernent les contrôles de cybersécurité sont orientées par les renseignements actuels sur les menaces, les pratiques exemplaires du secteur et la tolérance au risque de notre organisation.

c. Protection de la vie privée et des données

Nous respectons la vie privée de toutes les personnes et sommes déterminés à protéger les données sensibles. Les renseignements personnels et les renseignements personnels sur la santé sont gérés conformément à l'ensemble des lois et des normes applicables en matière de protection de la vie privée. Les pratiques de la SBCI sur le plan de la gouvernance des données ont été établies pour contrôler la façon dont les données sont recueillies, utilisées, stockées, communiquées et, éventuellement, éliminées. L'accès à des renseignements sensibles est limité aux personnes autorisées dont les fonctions l'exigent, et tout le personnel doit traiter ces genres de renseignements selon les paramètres de diligence les plus rigoureux.

d. Résilience et continuité

Nous tenons à renforcer la résilience de nos systèmes et de nos activités afin de veiller à offrir un service continu à nos parties intéressées. Notre infrastructure technologique est conçue pour éviter que des perturbations causées par des cyberincidents ou d'autres situations d'urgence ne se produisent, les supporter et s'en remettre rapidement. Nous tenons à jour nos plans d'intervention en cas d'incident ainsi que de continuité et de reprise des activités et les mettons régulièrement à l'essai afin que notre organisation puisse continuer à offrir des services essentiels malgré les difficultés.

e. Transparence et confiance du public

La SBCI reconnaît que la confiance est essentielle à nos relations avec le public et les parties intéressées. Nous nous engageons à maintenir cette confiance grâce à la transparence, à la reddition de comptes et à l'adoption d'un comportement éthique dans tous les volets de notre programme de cybersécurité. En cas d'incidents de sécurité d'envergure, nous communiquerons avec les parties concernées en temps opportun et de façon responsable, et nous collaborerons pleinement avec les organismes de

réglementation au besoin. Nous faisons également appel à des examens et à des vérifications externes pour fournir une garantie indépendante de notre position sur le plan de la sécurité.

f. Amélioration continue

Nous reconnaissons que le contexte de la cybersécurité évolue constamment, et le maintien de la sécurité passe par une vigilance constante. Nous surveillons les menaces émergentes, adaptons nos contrôles de sécurité au besoin et appliquons les leçons tirées des incidents, des évaluations et des vérifications pour renforcer nos moyens de défense. Nous investissons dans la formation et le perfectionnement continus de nos employés afin de maintenir une solide culture de sensibilisation à la sécurité et de responsabilité à l'échelle de l'organisation.

4. Gouvernance

Cette politique fait partie d'un cadre de gouvernance plus large et est appuyée par des normes, des procédures d'exploitation et des processus internes en matière de sécurité.

La surveillance de la présente politique relève du dirigeant principal des données et de l'information. Ce dernier est chargé d'assurer la mise en œuvre de la politique et la conformité à celle-ci. Le dirigeant principal des données et de l'information bénéficie du soutien du gestionnaire des opérations en matière de TI, du gestionnaire des applications de TI et du gestionnaire responsable de la gestion des données.

La présente politique fait l'objet d'un examen au moins une fois par année ou à la suite de l'opération de changements organisationnels ou technologiques importants afin de s'assurer qu'elle demeure efficace et respecte les pratiques exemplaires.

Terminologie

Contrôle d'accès : Techniques de sécurité qui déterminent qui peut visualiser ou utiliser les ressources dans un environnement informatique.

Données confidentielles : Renseignements de nature sensible qui doivent être protégés contre tout accès non autorisé (p. ex. données personnelles, financières ou exclusives).

Gouvernance des données : Cadre de politiques, de processus et de responsabilités qui permettent de veiller à ce que les données soient gérées de manière appropriée tout au long de leur cycle de vie.

Ressources numériques : Toute ressource technologique utilisée à des fins de création, de stockage, de traitement ou de transmission de renseignements, notamment le matériel, les logiciels, les services infonuagiques, les réseaux et les données électroniques.

Chiffrement : Processus de conversion des données sous forme codée pour empêcher l'accès non autorisé.

Renseignements personnels : Tout renseignement consigné au sujet d'une personne identifiable (p. ex. nom, adresse, numéro de téléphone et renseignements financiers).

Renseignements personnels sur la santé : Renseignements identificatoires sur la santé physique ou mentale, les antécédents médicaux ou la prestation de services de santé d'une personne.