CATEGORY	Information Technology	**DEPARTMENT CODE**	06
DOCUMENT #	002	**DOCUMENT TYPE**	Policy
DESCRIPTION	Cyber Security		
DATE APPROVED	December 2025	**NEXT REVIEW REQUIRED**	December 2028
LOCATION	*IT-06-PL-Cyber Security-002.docx*		

1. Purpose

At SBCI, the protection of school board data and the security of our systems are fundamental responsibilities. This Cybersecurity Policy defines the principles and commitments that guide our efforts to ensure the confidentiality, integrity, and availability of all information assets entrusted to us.

SBCI is committed to treating cybersecurity as a critical business priority, providing assurance to our members, partners, and interested parties that their information is handled with the highest level of care and security.

2. Scope

The policy applies to all digital systems, networks, applications, and data owned, operated, or managed by SBCI. It also applies to all employees, contractors, vendors, and third parties who have access to our digital resources3. Guiding Principles

a. Accountability and Leadership

SBCI views cybersecurity as a core organizational responsibility that requires active leadership and oversight. Executive management provides strategic direction, allocates resources, and oversees the implementation of our security framework. Roles and responsibilities for cybersecurity are clearly defined throughout the organization, ensuring accountability at every level. We promote a culture in which every staff member understands their role in safeguarding digital systems and protecting the information entrusted to us.

b. Risk Management

We follow a risk-based approach to cybersecurity, recognizing that not all threats pose the same level of impact. Risks are regularly assessed to identify potential threats, vulnerabilities, and their possible consequences on our operations and our members. This allows us to prioritize security investments and implement protective measures where they are most needed. Decisions about cybersecurity controls are informed by current threat intelligence, industry best practices, and our organizational risk tolerance.

c. Privacy and Data Protection

We respect the privacy of all individuals and are dedicated to protecting sensitive data. Personal Information (PI) and Personal Health Information (PHI) are handled in compliance with all applicable privacy legislation and standards. SBCI's data governance practices are in place to control how data is collected, used, stored, shared, and ultimately disposed of. Access to sensitive information is limited to authorized individuals whose duties require it, and all staff are expected to handle such information with the highest level of care.

d. Resilience and Continuity

We are committed to building resilience into our systems and operations to ensure uninterrupted service to our interested parties. Our technology infrastructure is designed to prevent, withstand, and recover quickly from disruptions caused by cyber incidents or other emergencies. We maintain and regularly test our plans for incident response, business continuity, and disaster recovery to ensure our organization can continue delivering essential services in the face of adversity.

e. Transparency and Public Trust

SBCI recognizes that trust is fundamental to our relationship with the public and our interested parties. We are committed to maintaining this trust through transparency, accountability, and ethical conduct in all aspects of our cybersecurity program. When significant security incidents occur, we will communicate with affected parties in a timely and responsible manner, and we will cooperate fully with regulatory authorities as required. We also engage external reviews and audits to provide independent assurance of our security posture.

f. Continuous Improvement

We acknowledge that the cybersecurity landscape is constantly evolving, and maintaining security requires ongoing vigilance. We monitor emerging threats, adapt our security controls as needed, and apply lessons learned from incidents, assessments, and audits to strengthen our defenses. We invest in the ongoing training and development of our employees to sustain a strong culture of security awareness and responsibility throughout the organization.

4. Governance

This policy forms part of broader governance framework and is supported by internal security standards, operational procedures, and processes.

Oversight of this policy rests with the Chief Data and Information Officer, who is responsible for ensuring its implementation and compliance. The Chief Data and Information Officer is supported by the IT Operations Manager, IT Applications Manager, and Data Management Manager.

This policy is reviewed at least annually or following major organizational or technological changes to ensure its continued effectiveness and alignment with best practices.

Terminology

Access Control: Security techniques that regulate who can view or use resources in a computing environment.

Confidential Data: Information that is sensitive and must be protected from unauthorized access (e.g., personal, financial, or proprietary data).

Data Governance: The framework of policies, processes, and responsibilities that ensure data is managed properly throughout its lifecycle.

Digital Resource: Any technology asset used to create, store, process, or transmit information. This includes hardware, software, cloud services, networks, and electronic data.

Encryption: The process of converting data into a coded form to prevent unauthorized access.

Personal Information (PI): Any recorded information about an identifiable individual (e.g., name, address, phone number, financial information).

Personal Health Information (PHI): Identifying information about an individual's physical or mental health, healthcare history, or provision of health services.