CYBERSECURITY HANDBOOK

Table of Contents

Principles

- Information and information systems are critical school board assets, like physical infrastructure and financial resources, and shall be safeguarded deliberately, appropriately and consistently throughout their life cycle.
- Cybersecurity shall be provided in a manner that serves the security and safety of students and staff while adhering to legislative requirements.
- Appropriate safeguards shall be in place to ensure the protection of students' and staff privacy and their safety online. The effort taken to apply those safeguards shall be proportionate to the possible harm or injury that could result if confidentiality, integrity and availability are not assured.
- All students and staff shall be informed of safe, responsible and ethical online behaviours and understand their accountability for the protection of information that is received, created, or maintained on behalf of the board.
- The school board, schools and all staff have a duty of care to take reasonable steps to protect students from harm encountered within the online learning environment.
- The Board aims to facilitate secure, safe, responsible and respectful use of technology as is further defined in the board's acceptable use of technology Administrative Procedures for Staff and Students (AUT) to support teaching and learning and prepare students for the risks and opportunities of the digital world, to thrive safely online, and become good digital citizens.

This document uses the following wording conventions:

Shall – The requirement is mandatory. Without it, the organization is not considered protected and deemed to be at a greater risk of cyber threats. If a mandatory requirement is currently not met, the board shall have a documented plan for remediating identified gaps.

Should – The requirement ought to be adhered to, unless there is a documented and approved business rationale for not adhering to it.

1. Cybersecurity Governance

1.1. A comprehensive board-wide Administrative Procedure on Cybersecurity shall be developed, implemented, communicated and maintained up to date.

1.2. The accompanying “Handbook” (this document) will be updated and reviewed with IT Services staff annually and with other stakeholders as part of the regular Administrative Procedure review process.

1.3. Comprehensive board standards, procedures and guidelines for cyber security, cyber safety and the protection of online privacy shall be developed, implemented, communicated and maintained up to date in accordance with the direction and priorities established by the board’s governance.

1.4. The board shall establish and maintain Cybersecurity as an integral part of the multi-year technology plan.

1.5. Authorized users shall comply with the Cybersecurity administrative procedure and the board’s Cybersecurity standards, procedures and guidelines, as applicable.

1.6. The board shall develop and maintain a catalog of board allowed applications and board staff shall only use applications identified in this catalog. Staff shall have the ability to request additions and changes to this catalog. All applications shall be subject to an application vetting process to assess privacy and data security risks, to determine inclusion or exclusion from the catalog.

2. Compliance with Legal and Ministry Requirements

2.1. The board’s Cybersecurity measures shall comply with all applicable laws, legislations and Ministry of Education policy directives.

3. Security of Sensitive Information

3.1. The board shall ensure individuals undergo personnel security screening commensurate to the duties they perform prior to being granted access to board sensitive information, information systems, and any board owned and managed IT or network-connected IT resources.

3.2. The board shall ensure authorized users of board IT and network connected OT resources:

3.2.1. Are aware of their Cybersecurity responsibilities;

3.2.2. Adhere to the board's Cybersecurity standards, procedures and guidelines as applicable to their role(s); and

3.2.3. Receive cyber protection awareness training to the extent necessary by their role(s) and level of access.

4. Cyber Risk Management

4.1. With increased reliance on technology, digital processes and the internet, the board recognizes that cyber risks have the potential to affect all aspects of the board, its staff and students, and reputation.

4.2. The board recognizes cyber risk management as an important practice that enables the board to align cyber security, cyber safety and digital privacy with board business objectives and business risk, ensuring the most effective and efficient way to mitigate against cyber risks.

4.3. As an integral part of cyber risk management, the board shall classify IT and network-connected OT assets to determine the level of information sensitivity and risk to the assets, and appropriate levels of safeguards needed to protect them. The classification level shall be determined by assessing the requirement for confidentiality of information, integrity and availability of information and systems.

4.4. Any new IT solution and network-connected OT solution in the board shall undergo an assessment of cyber risks prior to entering into a contract or service agreement, and prior to implementation. For cloud services, the assessment may be of evidence in the form of an attestation providing reasonable assurance regarding the presence and correct operation of safeguards within a service.

4.5. The board shall do a re-assessment of cyber risks if there are any significant changes to a board's IT solution, network-connected OT solution and/or the K-12 threat environment, and when deemed necessary.

4.6. All identified risks shall have a designation of who is responsible for their treatment, management and oversight with the Director of Education being ultimately accountable for all cyber risks in the board. Depending on the nature of the identified risk, responsibility for its risk treatment plan and its implementation may reside with the business owner, service owner, service provider or vendor.

4.7. The board shall monitor risk compliance for IT and network-connected OT resources deemed critical to the board. This may be done in the form of cyber risk assessments, penetration tests, vulnerability assessments, privacy impact assessments and other industry established practices.

5. Supply Chain, Cloud and Third-Party Service Providers

5.1. The board recognizes that cyber risks associated with a vendor's supply chain, third-party service providers, contractors, and cloud providers are important areas requiring coordinated risk mitigation efforts. Areas of third-party cyber risk include:

- 5.1.1. Access by third-party service providers or vendors - virtual or physical access to board technology, IT system and sensitive information.
- 5.1.2. Suppliers with poor cyber security and privacy protection practices.
- 5.1.3. Software, hardware and cloud services with vulnerabilities, compromised systems or embedded malware.
- 5.1.4. Cyber security vulnerabilities in supply chain management or supplier systems.
- 5.1.5. Third-party data storage or data aggregators.
- 5.1.6. Contract terms and conditions, including provisions around data privacy, incident response and the vendor's overall cyber security and privacy practices.

5.2. The board shall include cyber security, cyber safety and privacy requirements in technology procurements to ensure appropriate levels of information and user protection are in place.

5.3. The board shall institute cyber risk assessment practices as a key step in procurement of technology, cloud services and IT services to ensure adequacy of cyber security, cyber safety and privacy controls.

5.4. Contracts and service level agreements with third-party service providers (including any sub-contractors) who have access to or share custody of board information, IT systems, and/or other board technology shall include the obligation to follow the requirements of this policy and applicable board standards, procedures and guidelines, or be subject to equivalent industry-based assurances.

6. Availability and Reliability of Technology

6.1. The board shall define, for all business and time critical IT systems, business requirements and metrics for availability, reliability and continuity of service to inform business continuity and disaster recovery plans.

6.2. The board shall put in place, for all business and time critical IT systems, disaster recovery plans (DRP) to support continuity of business and timely recovery of IT systems in the event of a significant degradation of service or unplanned outage.

6.3. DRPs shall be the responsibility of IT and align with the Board's business continuity plan (BCP). The BCP shall help to define the business requirements for DRPs.
6.4. DRPs shall be periodically reviewed and maintained up to date to ensure plans can be successfully executed in the event of a disruptive event or major failure.
6.5. The board shall implement and periodically test backup and off-site storage procedures for all essential business information and critical IT systems no less than every 12 months, in the event data and IT systems need to be restored.

7. Network and Endpoint Security

7.1. The board shall implement reliable, enterprise-grade controls for the board network to regulate all traffic moving within the board network and between the board and external, untrusted (internet) entities (e.g. cloud service providers).
7.2. The board shall encrypt board sensitive data at rest and/or in transit as an important measure to mitigate against unauthorized access to information.
7.3. All board wireless access points, network connected devices, network-connected OT resources and internally or externally hosted applications (including cloud services) shall conform with board standards, procedures and guidelines.
7.4. Unauthorized wireless access points, connected devices, equipment, and remote connections (e.g. VPN or SSH tunnels) shall be scanned for and disabled on a regular basis.
7.5. The board shall not permit its networks to have open access except for managed guest networks that are isolated from the board's other network segments by reliable means.
7.6. The board shall implement protective measures and controls to monitor and secure endpoint devices and reduce the risk of cyber incidents and breaches from endpoint devices connected to the board network.

8. Incident and Breach Response Planning and Management

8.1. The board shall implement an incident and breach response plan(s) and incident and breach management procedure(s) that include definitions for metrics (e.g. severity levels, response timelines, etc.), terms used, accountability, roles and responsibilities, as well as protocols for detecting, containing, eradicating, recovering from and monitoring of cyber incidents and breaches as well as coordination, reporting, escalation procedures, and escalation contacts.

8.2. The board shall ensure users of the board's IT and network-connected OT resources are made aware of how to identify and report a cyber incident or breach.
8.3. Any person who causes or contributes to cyber incidents or breaches shall be held accountable when their actions contravene board standards, procedures and guidelines.

9. Monitoring

9.1. Board networks, devices / endpoints, systems / applications, network-connected equipment and platforms shall be monitored to detect and prevent potential cyber incidents and breaches in accordance with legislation.
9.2. Access to and analysis of monitoring data shall be restricted to authorized personnel only.

10. Vulnerability and Patch Management

10.1. The board shall create and maintain an asset inventory to track the board's IT and network-connected OT assets that need security/patching and to quickly identify, assess impacts and mitigate against vulnerabilities.
10.2. The board shall implement a patching and vulnerability management process to manage and mitigate board technology (software and hardware) vulnerabilities in the board's technology ecosystem. The process shall enable automatic patching for all technology or establish full vulnerability and patch management solutions to ensure technology are kept free of known vulnerabilities.

11. Access Control and Authorization

11.1. Board staff and any other individual requiring access to board sensitive information, IT systems and network-connected OT systems shall first be authorized through a board approval process. Access privileges shall be enough to enable an individual to perform their role but not permit them to exceed their authority.
11.2. Board user access shall be granted and/or terminated immediately upon receipt, and management's approval, of a documented access request/termination.
11.3. Board user accounts with elevated privileges shall be pro-actively monitored.

11.4. Auditing of access and usage for users' accounts shall be conducted regularly by the board to prevent privilege abuse.
11.5. The board shall implement multi-factor authentication (MFA) to control access to board sensitive data and systems.

12. Privacy and Data Protection

12.1. The board is committed to protecting the privacy of, and access to, students' and staff personal information held by the board and following rules for collection, use and disclosure as required by legislation
12.2. The board shall take appropriate measures to ensure the confidentiality, integrity and availability of sensitive information (including but not limited to board sensitive business information such as board financials, personal information (PI) and personal health information (PHI)).
12.3. All individuals with access to personal information and other board sensitive information shall be required to comply with applicable board policies, standards, procedures and guidelines, and abide by all applicable privacy laws and legislations.
12.4. The board recognizes the need to differentiate data from children (minors) and from that of adults, and that additional and/or different privacy safeguards may be needed for minors.

13. Cyber Awareness Training

13.1. The board shall conduct periodic cyber awareness training (on cyber security, cyber safety and online privacy) for authorized users of the board's IT resources and network-connected OT resources. Training shall be role-based and provide clarity on user responsibilities, where applicable in:
    13.1.1. Protecting board IT and network connected OT resources;
    13.1.2. Protecting privacy and confidentiality, and complying with regulations and legislation;
    13.1.3. Adhering to the board's Acceptable Use of Technology AP which includes expectations of appropriate online behaviour and the safe, responsible and secure use of board technology; and
    13.1.4. Adhering to board Cybersecurity standards, procedures and guidelines.

14. Exceptions

The board shall develop an exception request process that ensures any deviations to the policy and standards are remediated with an established timeframe. These exception requests shall be made to the Manager of IT and reviewed by the Manager of IT, Superintendent with responsibility for IT and Senior Administration as appropriate.

15. Contact

The main contact for the Cybersecurity Handbook is the Board's Manager of Information Technology.

Sean Heuchert
sheuchert@pvnccdsb.on.ca
705-748-4861 ext 1298

Any reporting for an actual or potential cyber incident should be made to the Board's IT Services Helpdesk:

helpdesk@pvnccdsb.on.ca
705-748-4861 ext 1281

Appendix A - Glossary

Access Privileges: authorized and controlled access to an information system from a pre-determined classification of set privileges, usually assigned by role (role-based access) or individual user (identity-based access).

Assets: Those resources (hardware, software, data etc.) associated with the creation, storage, processing and communication of information in the form of data, text, image or voice (i.e. Information assets, infrastructure assets and business application assets).

Asynchronous learning: Learning that is not delivered in real time. Asynchronous learning may involve students watching pre-recorded video lessons, completing assigned tasks, or contributing to online discussion boards.

Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

Availability: The degree of readiness expected of information systems and IT resources to deliver an appropriate and timely level of service, regardless of circumstances.

(Technology) Baselines: a more operationally focused form of a standard. The baseline defines a minimum level of Cybersecurity that must be met. For example, a board may choose one collaboration platform as its standard for all staff and educators. The IT department would subsequently configure this platform to a minimum baseline that ensures security and administration features are set to protect the platform.

Board Sensitive Information: Refers to school board data that must be protected from unauthorized access. It includes personal and confidential information about students and staff, and other board information such as financial data.

Breach: An information, security or privacy breach that compromises the confidentiality, integrity or accessibility of information or information systems

Business Continuity Plan: An action plan that defines alternate processes and facilities that would be used to enable critical information systems and resources to continue with planned degrees of interruption or essential change.

Cloud Service: A specific service offering and computing, networking, application, or storage function made available to users on demand via the Internet from a cloud service provider as opposed to being provided from an organization's own on-premise servers and equipment.

Confidentiality: Ensuring that information is accessible only to those authorized to have access. Unauthorized access to or disclosure of the information constitutes a loss of confidentiality. The protection of confidentiality must be consistent with the sensitivity of information and legislative requirements (e.g., MFIPPA, PHIPA).

Cyber Risk: a measure of the extent to which an entity is threatened by a potential circumstance or event, typically calculated by a consideration of the adverse impacts that would arise if a circumstance/event occurs, as well as the likelihood of it occurring.

Cyber Risk Management: is the ongoing process of identifying, assessing, and responding to risk associated with technology, the internet and the reliance on digital processes and services to run the business.

Cyber Safety: Impacts the human side and relates to safe practices to mitigate against inappropriate use and conduct online. This is especially important in the K-12 education sector.

Cybersecurity: Cybersecurity consists of standards, processes, procedures and tools organizations use to protect computers, servers, devices, networks, applications, IT systems, software and information from cyber threats, cyber threat actors, malicious cyberattacks and unauthorized access.

Cyber Threat: A cyber threat is a circumstance or event with the potential to adversely impact or compromise the security of an organization's IT systems and digital information. Examples include unauthorized access, destruction, disclosure, modification of information, and/or denial of service or system outages.

Cyber Threat Actors: A cyber threat actor are states, groups, or individuals (some very well organized and well-funded) who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to IT systems in order to access or otherwise affect victims' data, devices, systems, and networks.

Disaster Recovery Plan: Detailed steps necessary to recover information, information systems and resources at an alternate site.

Endpoint Device: general term that refers to any network-connected hardware device (e.g. smartphone, laptop, Internet-of-Things (IoT), etc.).

Elevated Privileges: Enhanced rights and/or administrative control, assigned to a user, over a particular IT resource or class of resources.

Information Technology (IT) System: is defined as any electronic system that stores, processes, or transmits information.

Integrity: The quality of authenticity, accuracy and completeness for data, which can be adversely impacted by unauthorized or accidental additions, changes and/or deletions.

Mitigate: A term related to risk management meaning the reduction of the severity of the impact or likelihood of a risk or an event.

Monitor: The process of collecting and analyzing information, on a regular basis, to check, supervise, observe critically, or track/record the progress of an activity, action, program or system towards desired outcomes.

Operational Technology (OT): Refers to network-connected equipment (hardware and software) used to change, monitor, or control physical devices and equipment such as building management systems, building automation systems, facilities sensors, HVAC (Heating, Ventilation and Air Conditioning) systems and SCADA (Supervisory Control and Data Acquisition) systems.

Personal Information (PI): MFIPPA defines personal information as recorded information about an identifiable individual. It includes information such as name, address, phone number, school photos, videos, health information and student records.

Privacy Breach: (as defined by MFIPPA) Means an incident where personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with personal information protection requirements in statute and regulation.

Privacy protection: Related to measures implemented to protect personal information from unauthorized access.

Procedures: Detailed step-by-step documents that describe the exact actions necessary to implement and/or operate specific Cybersecurity mechanisms, controls or solutions. Procedures are typically process or system specific and ensure the integrity of the process / system. Some organizations may refer to these as Standard Operating Procedures (SOPs), Administrative Procedures or other name. Some organizations may have different categories of procedures and different approval levels for each category.

Remote learning: Learning that occurs when classes are taught at a distance and when students and educators are not in a conventional classroom setting. Remote learning takes place in times of extended interruption to in-person learning – for example, as a result of a pandemic or natural disaster. Classes can be synchronous or asynchronous and can be taught online through a Learning Management System (LMS) or by using videoconferencing tools. In some cases, they may be delivered through emails, print materials, broadcast media, or telephone calls. *Definition from PPM 164*[1]

Safeguard: A protective and precautionary measure intended to prevent a cyber threat from happening or a threat agent from causing harm and injury.

Significant Change: A significant or major change are those that have the potential to impact either many users or a critical board service or business function, either as part of the change implementation or as a result of a high-risk change failure.

Standards: A specification for hardware and software solutions, or mandatory requirements or actions (as may be documented in processes and/or procedures). For example, board-provided devices may have standard images that include prerequisite software and setup/configurations. Educators may be required to use specific applications when teaching in the classroom such as Microsoft Teams, Google Classroom, Zoom and other education technology tools. These may also need to be configured with specific parameters to ensure protection of privacy and mitigation of online threats.

Synchronous learning: Learning that happens in real time. Synchronous learning involves using text, video, or voice communication in a way that enables educators and other members of the school- or board-based team to instruct and connect with students in real time. Synchronous learning supports the well-being and academic achievement of all students, including students with special education needs, by providing educators and students with an interactive and engaging way to learn. It helps educators provide immediate feedback to students and enables students to interact with one another. *Definition from PPM 164*[2]

---

[1] http://www.edu.gov.on.ca/extra/eng/ppm/164.html
[2] http://www.edu.gov.on.ca/extra/eng/ppm/164.html

Technology Ecosystem: The collection of technology solutions that an organization uses to run its business. This includes but is not limited to computers, servers, mobile devices, networks, applications, information systems, software, education applications and tools, the internet, internet connected equipment (e.g. IoT), and digital information.

Appendix B - References

PVNCCDSB Administrative Procedures Related to Cybersecurity

Directional Policy 300 - Student Achievement and Well-Being

AP 313 - Student Acceptable Use of Technology
AP 314 - Personal Network Devices
AP 322 - Digital Privacy

Directional Policy 500 - Employee Relations

AP511 - Employee Acceptable Use of Technology
AP516 - Use of Electronic Communications and Social Media

Directional Policy 600 - Stewardship of Resources

AP 610 - Purchasing
AP 615 - Emergency Management and Business Continuity Program
AP 602 - Cybersecurity