Greater Essex County District School Board

Title: Cyber Security
Category: Operational Procedure
Department: Information Technology
Responsibility: Superintendent of School Operations and Information Technology
Effective Date: April 21, 2020
Review Date: June 2, 2026
Next Review Year: 2031

Rationale

The Greater Essex County District School Board (GECDSB) recognizes the critical importance of cyber security in protecting the integrity, confidentiality, and availability of its information technology resources. Cyber security involves defending IT resources from unauthorized access, use, disclosure, disruption, modification, and destruction, while ensuring that controls are proportionate to risk (for example, phishing, hacking, and password compromise).

The Board is committed to ensuring that all activities involving information technology resources are appropriately defended against cyber security threats. Successful cyber security depends on a well-informed user community combined with effective management procedures and a shared responsibility for protecting the Board's IT environment.

This Operational Procedure applies to all employees, students, families, volunteers, visitors, contractors, trustees, and any other individuals authorized to access GECDSB Information Technology Resources. All individuals acting on behalf of the Board share responsibility for cyber security.

Guiding Principles:

- All Board IT resources will be protected and monitored through the effective management of cyber security risks by all users.
- A cyber risk assessment will be performed at the start of every digital initiative to ensure that risk controls are identified, considered, and continued through the life cycle of service delivery.
- Cyber security incident response and recovery plans must be coordinated, maintained, and tested with internal and external stakeholders.
- The effectiveness of the Board's management of cyber security risks must be regularly assessed and improved or refined as necessary.
- All access to Board IT resources must be authorized, restricted based on need, and regularly verified.
- All users have a shared responsibility for maintaining the security of Board IT resources that they use or manage (see Digital Responsibility, R-IT-03).

- Users must not communicate the Board's cyber security risks, events, controls, or incidents outside the Board, except where required or authorized by law, Board policy, or applicable technical standards.

Definitions

Cyber Security
The efforts to design, implement, and maintain the security of IT resources.

Cyber Security Events
Any occurrence in an IT resource that has, or may potentially have, the effect of interfering with or impeding achievement of the Board's goals or objectives.

Cyber Security Risk
Exposure to harm or loss resulting from breaches of, or attacks on, IT resources.

Information Technology Resources (IT Resources)
IT resources include, but are not limited to: computers, phones, tablets, cellular and mobile technology, applications, email, Internet of Things (IoT) devices, servers, networks, internet services, internet access, data, websites, and any other electronic or communication technology provided by GECDSB or by a third party that exists today or may be developed in the future, regardless of whether it is used as a stand-alone device.

Risk Mitigation
The process of planning for cyber events and having a process in place to lessen their negative impact.

System Owner
An employee with primary accountability for the business or technology functions provided by one or more Board IT resources, including any associated cyber security risk.

Users
Users include, but are not limited to: staff, students, families, volunteers, visitors, contractors, trustees, and any other authorized individuals provided access to GECDSB Information Technology Resources.

Procedure

1. Roles and Responsibilities

Cyber security is a shared responsibility. The following describes the specific accountabilities of senior leadership, IT Services management, system owners, and all users of Board IT resources.

1.1 Director's Council

The Director's Council is accountable for approving the overall management of cyber security risk at the Board. Responsibilities include:

- Approving the Board's cyber security risk acceptance and tolerance levels.
- Considering and responding appropriately to the Board's cyber security risks and their management.
- Promoting an appropriate cyber security risk management culture across the Board.
- Overseeing the allocation of resources to enable effective cyber security risk management.

1.2 Superintendent of Information Technology Services

The Superintendent of Information Technology Services is responsible for:

- Overseeing security risk acceptance and tolerance levels.
- Receiving and acting on reports of cyber security risk management issues from Information Technology Services.
- Raising cyber security risk management issues with the Director of Education and/or the Director's Council, where appropriate.
- Communicating cyber security risk management issues with all staff, as appropriate.

1.3 Manager of Information Technology Services

The Manager of Information Technology Services is responsible for:

- Managing cyber security risks within the Information Technology Services department and assigning risk owners.
- Implementing the cyber security framework.
- Managing cyber security resources.
- Determining technical standards and assigning management responsibility for cyber security.
- Overseeing the design and implementation of the Board's cyber security plan, controls, and capabilities.
- Reviewing and reporting on the management of cyber security risks.
- Determining the cyber security related services required to support the Board's cyber security strategy, strategic priorities, legal and contractual obligations, and related policies and procedures.

1.4 System Owners

System Owners are responsible for:

- Working with Information Technology Services to perform a cyber risk assessment at the start of any new digital initiative or upgrade to existing systems.
- Complying with this Operational Procedure, related Board policies, administrative procedures, and applicable technical standards.
- Managing cyber security risks associated with the IT resources and third-party service providers under their charge.
- Immediately reporting any known or suspected cyber security incidents or breaches to the Cybersmart Helpline at extension 41199.

1.5 All Staff and Students Using Information Technology Resources

All staff and students using IT resources are responsible for:

- Following Board IT policies and procedures at all times while using IT resources.
- Being aware of the security requirements of the IT resources they use.
- Taking every precaution to safeguard their access to Board systems against unauthorized use (for example, not sharing passwords and not leaving workstations unlocked).
- Immediately reporting any known or suspected cyber security incidents or breaches to the Cybersmart Helpline at extension 41199.

2. Authorized Access

Only authorized users are permitted to access the Board's Information Technology Resources. Access must be requested, granted, and managed in accordance with established Board procedures, and is to be restricted based on demonstrated need and reviewed on a regular basis.

3. Reporting Cyber Security Incidents

Any individual who becomes aware of, or reasonably suspects, a cyber security incident or breach must report it without delay. Reports may be made to:

- The Cybersmart Helpline at extension 41199 (preferred for all incidents).
- In the case of staff, their immediate supervisor.
- In the case of students, their teacher or supervising staff member, who must promptly report the incident to the Principal or Vice-Principal.
- In the case of all other authorized users, the ITS Help Desk.

4. Cyber Risk Assessment

Information Technology Services, in collaboration with system owners, will perform a cyber risk assessment at the start of any new digital initiative or significant upgrade to an existing system. Identified controls will be implemented and maintained throughout the service life cycle.

5. Incident Response and Recovery

The Board will maintain documented cyber security incident response and recovery plans. These plans will be coordinated with internal and external stakeholders and will be tested on a regular basis to confirm their effectiveness.

6. Confidentiality of Cyber Security Information

Users must not communicate the Board's cyber security risks, events, controls, or incidents outside the Board, except where required or authorized to do so by law, or as stated in or following Board policies, procedures, or applicable technical standards.

7. Review and Continuous Improvement

This Operational Procedure will be reviewed periodically to ensure it remains effective, current, and aligned with best practices, legislative requirements, and related GECDSB policies. Reviews may be informed by audit findings, incident reviews, changes in legislation, or emerging cyber security risks.

Reference

Board Documents:

- Digital Responsibility
- Network Security and Access
- Privacy of Information
- Records Management
- Code of Conduct

Where a conflict exists between this Operational Procedure and another Board policy or procedure, the more stringent control or requirement shall apply.