SUPERIOR-GREENSTONE DISTRICT SCHOOL BOARD

Section	PROGRAM	612

Policy Name	IT CHANGE MANAGEMENT POLICY

Board Approved: November 16, 2021	*Review Prior To: December 2026*

OBJECTIVE

The objective of this policy is to define formal requirements to manage changes to IT systems and applications, in order to prevent unscheduled disruption of service delivery, data corruption, data loss, breaches of information governance, or the introduction of security vulnerabilities.

POLICY

The SGDSB formally manages changes to its Information Technology ("IT") resources to prevent disruptions to the stability or integrity of the board's IT systems, applications, and data.

DEFINITIONS

"validated" means that a detailed plan exists, has been reviewed by qualified people with the necessary subject matter expertise, and approved by an authority responsible for governing the process.

"authorized" means that an authority responsible for ensuring that this policy is adhered to has performed their duties.

"verifiable" means the ability to prove that the intended outcome will be achieved upon the successful completion of intended changes.

"risk managed" means that potential negative consequences of making the change have been identified, assessed, and mitigation plans formulated where appropriate. It also means the inclusion of a process to follow if the change needs to be undone and the systems returned to their former state.

"service delivery" means information technology hardware, systems, and networks that are relied upon to maintain operational capability of the organization.

JUSTIFICATION

Uncontrolled changes to IT systems and applications could potentially result in significant system disruption, data corruption or loss.

A formalized IT change management process is designed to ensure that proposed changes are validated and authorized, while authorized changes are clearly articulated, scheduled, verifiable, and risk managed.

SCOPE

This policy applies to:
1. All IT systems or applications managed by the SGDSB that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

2. All change requests made to IT.

EXCEPTIONS

Exceptions to the guiding principles in this policy must be documented and formally approved by the Manager of IT Services, with evidence of support from the appropriate Vice-President.

Policy exceptions must describe:
1. The nature of the exception including:
    a. A reasonable explanation for why the policy exception is required.
    b. Any risks created by the policy exception.
    c. Evidence of approval by the Manager of IT Services.

INQUIRIES

Inquiries regarding this policy can be directed to the Manager of IT Services.

POLICY METADATA

Responsibility	IT Manager
Review Schedule	Every 5 Years

REFERENCES

Document	*Description*	*Location*
IT Change Management Process	Document encapsulating how this policy is to be implemented.	