OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Appendix C to COW 18
February 2020

POLICY P.074.IT

TITLE: *INFORMATION TECHNOLOGY* SECURITY

Date Issued: February 1999
Last Revised: *18 February 2020*
Authorization: Board: 27 January 1999

1.0 OBJECTIVE

To ensure the safety, security, ***accessibility, confidentiality,*** integrity, and business continuity of ***information technology*** systems to protect the information ***created,*** owned, processed, or transmitted electronically by the Ottawa-Carleton District School Board.

2.0 DEFINITIONS

In this policy,

2.1 **Access** means direct or indirect use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer or other electronic device, computer system, facility or network.

2.2 **Authorization** means 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 consistent with the authorized consent or permission.

2.3 **Availability** means that systems, applications and data are available to users when they need them;

2.4 **Board** means the Board of Trustees.

2.5 **Computer** refers to any electronic device or communication device that stores, retrieves, processes, or transmits data.

2.6 **Computer system** refers to a set of related, connected or unconnected, devices, software, or other related computer equipment.

2.7 **Computer network** means the interconnection of computers, electronic devices, software, or other equipment.

2.8 **Computer property** includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

2.9 **Confidential** means data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

2.10 **Digital assets** refers to any form of information received, created or gathered on behalf of the OCDSB in the course of District business.

2.11 **District** means the Ottawa-Carleton District School Board.

2.12 **Encryption or encrypted data** refers to the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

2.13 **Information** means all information holdings that are stored, transmitted, or processed electronically in the course of District business.

2.14 ***Information Technology*** refers to a computer, device, or network on which there is a significant operational dependency for the District, and/or which stores, transmits, or provides access to sensitive information. This can refer to computers functioning as servers, and storage devices such as USB keys and portable hard drives, personal computers, printers, and photocopiers which have internal storage capability that could contain sensitive information.

2.15 **Infrastructure** refers to the set of information technology components that are the foundation of information technology services; typically physical components, but also various software and network components

2.16 **Integrity of information** means safeguarding information from unauthorized alteration or destruction.

2.17 **Physical Assets** refers to the information technology infrastructure, such as computers, devices, software applications, network equipment and peripherals, encryption devices, etc. used in the processing, storage, and transmittal of information.

2.18 **Privacy refers** to the quality or condition of being secluded by the presence or view of others. The state of being free from unsanctioned intrusion: a person’s right to privacy.

2.19 **Security system** refers to access control technologies such as encryption, password protection, and other forced authentication or access controls designed to keep out unauthorized persons.

2.20 **Security Threats** refers to any possible danger that might exploit a vulnerability to breach security safeguards and therefore cause possible harm to the District’s information and/or physical assets.

2.21 **Sensitive information** refers to an electronic set of information or data, such as a database, file or document, that is classified as personal or confidential, whether it is stored on or off premises.

2.22 **Third Party** refers to external vendors or contractors which provide supporting services to the District.

3.0 GUIDING PRINCIPLES

3.1 The Board believes that:

a) a strong, reliable, and secure information technology infrastructure is essential to ensuring an effective working and learning environment;

b) a secure infrastructure includes effective long-term contingency and incident management planning to prevent, manage and quickly recover from a security threat or any incident and reduce risk to the organization; and

c) where data ***is*** shared with third parties, they ***must*** maintain the confidentiality, integrity and security standards of the ***District***

d) systems and data will be secured by assigned and appropriate access to assure the confidentiality, integrity and security of assets; and

e) a governance structure ***as well as appropriate life-cycle asset management and investment are*** critical to promote risk management and ***the*** long term security ***of the board's information technology systems.***.

3.2 Physical and digital assets are corporate assets and ***are*** considered property of the OCDSB.

4.0 SPECIFIC DIRECTIVES

4.1 All users of the District network including staff, trustees, parents, students, vendors, consultants, and partners, with OCDSB-owned and personal assets under their control shall:

a) safeguard the confidentiality, integrity and availability of District physical and digital assets preserving the privacy of electronically maintained personal information in the custody or control of the District, whether stored on premises or external to the District;

b) make ethical choices that abide by the parameters of the Appropriate Use of Technology Procedure when utilizing assets;

c) identify and report all suspected or confirmed security incidents in accordance with procedures for reporting information technology or information security incidents or risks;

d) monitor and enforce compliance with this policy within the scope of their duties and responsibilities.

4.2 The District shall make every reasonable effort to protect and secure ***digital*** and ***physical*** assets from threat, abuse and/or misuse, including through human error, hardware malfunction, natural disaster, security breach, and/or malicious attack.

<u>Security Safeguards</u>

4.3 The District shall ensure the security of all information technology through~~:~~ classification, control, **and** technical measures ***to ensure*** its use is in accordance with Board policy.

4.4 The District shall have a formalized incident management, monitoring, compliance and business continuity response plan in place, aligned with Emergency Response Protocols.

<u>Implementation</u>

4.5 The Director of Education is authorized to issue procedures to ensure Information Technology security is integrated with all aspects of the operations of the District.

5.0 REFERENCE DOCUMENTS

The Education Act, 1998, ss. 170, 171
Board Policy P.027.GOV: Corporate Records Management
Board Policy P.049.IT: Electronic Communications Systems
Board Policy P.100.IT Appropriate Use of Technology
Board Policy P.128.GOV Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Board Procedure PR.516.GOV Corporate Records Management Board
Procedure PR.564.IT Computer Network Security
Board Procedure PR.622.IT Appropriate Use of Technology
Board Procedure PR.669.GOV Privacy Breach
Board Procedure PR.672.IT Electronic Communications Systems
Board Procedure PR.685.IT Mobile Devices
NIST Cyber Security Framework 1.1
ISO/IEC 27001:2013