APPENDIX G

Information Technology Security Procedure

Procedure Number:	5017a
Procedure Owner:	Information Technology Services
Effective Date:	2013 November 12
Amendment Dates:	2015 November 10 Replaced Procedure #9003 Technology Security Procedures (1998 December 11, 2001, June 13, 2002 February 26, 2007 November 13, 2008 May 27)
EIE Review Date:	2024 December 18
Resources:	• TVDSB Information Technology Policy (5017) • TVDSB Information Technology Appropriate Usage and Electronic Monitoring Procedure (5017b) • Municipal Freedom of Information and Protection of Privacy Act • Ontario Human Rights Code • Canadian Charter of Rights and Freedoms • Canada's Anti-Spam Legislation (CASL) • TVDSB Privacy and the Management of Personal Information Procedure (2014b)

1. Intent

1.1. This procedure specifies the steps Thames Valley District School Board (TVDSB) will take to safeguard its Information Resources and ensure appropriate usage of these resources.

2. Definitions

2.1. **Business Continuity** refers to the ability of an organization to maintain essential functions and operations during and after a disruptive event, such as a natural disaster, cyberattack, or system failure. In technical terms, business continuity involves the creation of a Business Continuity Plan (BCP), which includes strategies for data backup, system redundancy, disaster recovery, and alternative communication methods. It focuses on minimizing downtime, ensuring access to critical applications and services, and maintaining the integrity of business processes.

2.1. **Cyber Awareness** is the knowledge and understanding of potential cyber threats, such as phishing, social engineering, and data breaches. It involves staying informed about the latest cyber threats that TVDSB and its information resources face every day, following cyber protection best practices, and recognizing the risks associated with common internet activities.

2.2. **Cyber Incidence Response Plan** is the set of procedures that combines TVDSB processes, resources and technologies for detecting and responding to cyber threats, security breaches or cyberattacks.

2.3. **Cyber Protection** is the term used to collectively describe Cyber Security, Cyber/Online Safety and Digital/Online Privacy.

2.4. **Cyber/Online Safety** refers to the promotion of safe online practices and the mitigation of the risks associated with the inappropriate use of technology in accordance with TVDSB's Appropriate Usage and Electronic Monitoring Procedure.

2.5. **Cyber Security** refers to the protection of information and information technology resources with respect to confidentiality, availability and integrity, and secure network-connected technology resources.

2.6. **Cyber Threat** is any malicious act that seeks to damage data, steal data, disrupt digital life in general or impact TVDSB operations. Cyber threats include computer viruses, malware, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

2.7. **Data Loss Prevention (DLP)** is a set of strategies and tools used to protect sensitive information from being accidentally or intentionally lost, stolen, or exposed. It helps ensure that important data, like personal details, financial information, or confidential documents, doesn't leave the company or organization without permission. DLP can track, monitor, and block any attempts to transfer or access this sensitive data in ways that could put it at risk.

2.8. **Digital/Online Privacy** refers to the protection of personal information, personal health information, and other TVDSB sensitive information from unauthorized access, and recognizes the importance of guarding personal and sensitive information when using technology.

2.9. **Disaster Recovery Plan (DRP)** is a comprehensive set of procedures and strategies designed to restore IT systems, applications, data, and infrastructure after a disruptive event, such as hardware failure, cyberattack, or natural disaster. It outlines the processes for backing up data, recovering servers, re-establishing network connectivity, and ensuring business continuity with minimal downtime.

2.10. **Information Resources** include but are not limited to TVDSB's information technology services, TVDSB assigned email and network accounts, electronic data, application systems, facilities, wired and wireless networks, and technology equipment and infrastructure that TVDSB owns, operates, or sources from external parties, for the use of students, employees and other authorized users.

2.11. **Multi-Factor Authentication (MFA)** is a security process that requires two or more types of identification before access to an account or system is provided This adds extra layers of protection to make it harder for someone to access a user account.

2.12. **Penetration Testing** is a "security check-up" for computer systems or networks. It involves simulating a cyberattack to find weaknesses or vulnerabilities that could be exploited by hackers. Skilled testers try to "break into" the system, just like a real attacker would, to see where the security could be improved. This helps organizations fix potential problems before a real threat can take advantage of them.

2.13. **Personal Information (PI)** refers to recorded information about an individual that

renders that individual identifiable. PI includes name, address, phone number, race, ethnic origin, religious or political beliefs or associations, age, sex, sexual orientation, mental status, family status, any identifying number or symbol such as Social Insurance Number (SIN), fingerprints, blood type, or inheritable characteristics, medical history, educational, financial, criminal, or employment history, personal views or opinions, except if they are about someone else; or anyone else's opinion about that individual.

2.14. **Service Level Agreement (SLA)** is a contract between a service provider and TVDSB that outlines the services to be provided, how performance will be measured, and what happens if the service provider doesn't meet their obligations.

2.15. **Single Sign-On (SSO)** is an authentication method that allows users to log in to multiple applications and websites with one set of credentials. Once logged in to one system, users are automatically authenticated for other connected systems without needing to re-enter their login credentials.

2.16. **Software Applications and Systems** safeguard the online privacy and security of students and staff, TVDSB has implemented an approval process to ensure all digital resources meet stringent criteria for safety and educational relevance. The approved resources listed in the Approved Software and Websites have undergone comprehensive evaluation based on their alignment with curriculum objectives, as well as adherence to strict standards for security and privacy protection.

2.17. **Threat Landscape** is a comprehensive overview of all known and potential cyber threats that could affect TVDSB Information Resources, student, employee and other authorized TVDSB users. It includes both current and historical threats, as well as emerging trends, vulnerabilities and exploits.

2.18. **Virtual Private Network (VPN)** establishes a digital connection between a computer and a remote server, creating a point-to-point tunnel that encrypts data, masks an IP address, and avoids website blocks and firewalls on the Internet.

2.19. **Vulnerability Assessments** are a process of checking and identifying weaknesses or security gaps in a computer system, network, or software. The goal is to find areas that could be exploited by hackers or lead to problems like data breaches or

system failures. Once these weaknesses are found, steps can be taken to fix or improve them, making the system safer and more secure.

2.20. **Commercial Electronic Message** encourage participation in a commercial activity, including:

2.20.1. Offers to purchase sell, barter or lease a product, goods, a service, land or an interest or right in land

2.20.2. Offers to provide a business, investment or gaming opportunity.

2.20.3. Advertises or promotes anything referred to in (a) or (b); or

2.20.4. Promotes a person, including the public image of a person, as being a person who does anything referred to in (a) or (c), or intends to do so.

Commercial electronic message can be sent via email, SMS text message or instant messaging. It does not include two-way voice communication, a fax, a telephone voice recording, a social media post or a website post.

2.21. **Commercial Activity** means any particular transaction, act, or conduct or any regular course of conduct that is of a commercial character, whether the person who carries it out does so in expectation of profit.

Exclusions under the Act include commercial activities for the purposes of law enforcement, public safety, protection of Canada, the conduct of international affairs, the defense of Canada, soliciting contributions for a political party/organization/candidate, or fundraising by a registered Canadian charity.

3. Objective of Procedure

3.1. The following objectives help create a secure and resilient Information Technology (IT) environment that supports the educational mission of TVDSB while protecting the privacy and safety of all students and staff.

3.1.1. Protecting Student and Staff Data: Safeguarding personal and sensitive information from unauthorized access, breaches, and cyber threats.

3.1.2. Ensuring Cyber Safety: Promoting safe online practices and the mitigation of the risks associated with the inappropriate use of technology in

accordance with the TVDSB's Information Technology Appropriate Usage and Electronic Monitoring Procedure.

3.1.3. Compliance with Regulations: Adhering to local, provincial and federal laws, as well as TVDSB guidelines and educational standards, to ensure legal and ethical management of data.

3.1.4. Cyber Incident Response: Establishing protocols for responding to cyber incidents, including detection, reporting, and remediation.

3.1.5. Cyber Risk Management: Identifying, assessing, and prioritizing risks to minimize, monitor, and control the probability or impact of adverse events.

4. Roles and Responsibility

4.1. **Staff Supervisors** are accountable for ensuring staff are informed of the procedures and that compliance occurs. All staff members and Trustees are required to complete an annual declaration acknowledging awareness of and the need for compliance with the Information Technology Policy and underlying procedures.

4.2. **Information Technology Services (ITS) Department** will configure, maintain and manage the Information Technology (IT) infrastructure and Information Resources entrusted to its care in accordance with departmental protocols. The ITS department shall establish and maintain cyber protection initiative for implementing and improving cyber security across TVDSB.

4.3. **Contracts and service level agreements** (SLA) with third party service providers who have access to or share custody of the TVDSB Information Resources shall include the obligation to follow the requirements of this procedure as applicable. This shall extend to any subcontractors on whom the service providers rely on to deliver services to TVDSB.

4.4. **All users of TVDSB Information Resources** are responsible for ensuring that these resources and the data owned by TVDSB are used exclusively to support TVDSB objectives and in compliance with all applicable local, provincial and federal laws, guidelines and directives. Failure to comply with this Procedure will result in

disciplinary action that may include dismissal.

5. Information Technology Security Procedures

5.1. With increased reliance on technology, digital processes, and the internet, TVDSB acknowledges that cyber risks can impact all aspects of the organization, including its staff, students, and reputation. Cyber risk management is a crucial practice that aligns cyber security, cyber safety, and digital privacy with its strategic priorities and operational plan initiatives.

5.2. The following sections will outline TVDSB's essential protocols to Information Technology Security, planning and awareness, access and authentication, devices, applications and monitoring.

6. Essential Protocols for Information Technology Security

6.1. ITS Department will implement reliable, enterprise-grade controls for TVDSB network to regulate all traffic within TVDSB network and between TVDSB and external, untrusted entities (e.g., cloud service providers). Additionally, ITS Department will implement protective measures and controls to procure, monitor, and secure endpoint devices.

6.2. ITS Department will implement Data Loss Prevention capabilities to identify, monitor, and protect data in use, in motion, and at rest. Under no circumstances should an employee transfer or back up TVDSB data from their account to a non-TVDSB account.

6.3. When working remotely, TVDSB Information Resources must be treated as confidential and must not be exposed to unauthorized parties, including individuals such as family members.

6.4. ITS Department will implement technologies and policies to block unsolicited and irrelevant electronic messages (such as spam) from accessing the TVDSB email system. Additionally, ITS Department will adjust the current electronic messaging systems, as needed, to restrict bulk commercial messaging originating from the TVDSB network. TVDSB will ensure that the list of approved software identifies and includes software that complies with Canada's Anti-Spam Legislation (CASL) for the

purposes of sending commercial electronic messages.

7. Planning and Awareness

7.1. ITS will categorize IT equipment and resources based on their information sensitivity and associated risks. This classification will help determine the necessary safeguards to protect these resources.

7.2. ITS will assess and reassess cyber risks if there are significant changes to TVDSB information technology solutions, or the threat landscape, or when deemed necessary. Depending on the nature of the identified risk, responsibility for its treatment plan and implementation or remediation may reside with ITS, another department, service area, or external third party.

7.3. ITS will use a combination of vulnerability assessments, penetration testing and other industry practices to monitor, assess, test, and address issues related to the security of TVDSB Information Resources.

7.4. For all business and time-critical IT systems, ITS will implement and review its DRP to support business continuity and timely recovery of IT systems in the event of significant service degradation or unplanned outage.

7.5. ITS will ensure that users of TVDSB information technology resources are aware of how to identify and report a cyber incident or breach.

8. Access and Authentication

8.1. In collaboration with Human Resources (HR), ITS will ensure that new hires and individuals in new positions or roles at TVDSB are assigned appropriate privileges, granted access, and provided with security training relevant to their duties before they are given access to TVDSB Information Resources.

8.2. At the time of retirement, resignation, leave, or termination of employment, HR will collaborate with ITS to ensure timely processes are in place to retrieve TVDSB devices as required and disable access to TVDSB accounts and resources.

8.3. TVDSB will ensure regular, and ongoing cyber awareness and data protection training for TVDSB users is provided.

8.4. TVDSB will implement identity and access management programs to ensure that only authorized individuals have access to TVDSB Information Resources.

8.5. ITS will facilitate and prioritize employee SSO functionality wherever possible subject to security, software and operational limitations.

8.6. All sta□ users will be required to authenticate using an approved MFA application as the primary means of personal authentication.

8.7. All TVDSB wireless access points, network-connected resources, and internally or externally hosted applications (including cloud services) must conform to TVDSB standards, procedures, and guidelines. Unauthorized networks, access points, and unapproved communication tools at TVDSB schools and sites, including unapproved wireless access points, connected devices, equipment, and remote connections.

8.8. Unauthorized wireless access points, connected devices, equipment, and remote connections will be disabled upon discovery.

8.9. ITS Department is responsible for configuring managing and administering all TVDSB wired and wireless networks. Access to these networks will be restricted to authorized users.

9. Devices

9.1. Only trusted individuals and devices will be permitted to access TVDSB Information Resources.

9.2. Only devices configured and managed through ITS will be permitted on any secured TVDSB infrastructure. Devices that are not configured and managed through ITS and/or do not meet a minimum-security standard will not be allowed to operate on any secured TVDSB infrastructure and will not have access to any data, applications, and systems.

9.3. ITS will maintain an asset inventory to track, administer, replace and report on TVDSB technology infrastructure.

10. Applications

10.1. TVDSB shall take appropriate measures to ensure the confidentiality, integrity, and availability of software applications and systems. Any software applications and systems that do not meet TVDSB standards for privacy, security, and/or data protection, as determined by ITS, will not be authorized for use by students and/or staff.

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

10.3. All software must undergo a vetting review process prior to installation to evaluate its pedagogical value, technical compatibility, privacy risks, and security concerns. TVDSB staff are required to use only those applications and software listed in the TVDSB approved software list. Any applications or technologies not included in this approved catalogue are prohibited for use by staff and students on TVDSB devices or infrastructure.

11. Network Monitoring

11.1. TVDSB shall ensure process and applications are used to monitor any and all of the aspects of its Information Resources, including, without limitation, reviewing documents created and stored on its computer system, deleting any matter stored on its Information Resources, monitoring websites visited by Users, monitoring chat and news groups, reviewing all material downloaded or uploaded by Users from the Internet, and reviewing e-mail sent and received by Users.

11.2. ITS will employ automated detection and response capabilities to monitor, detect, and remediate potential or actualized cyber incidents and breaches on TVDSB networks, devices/endpoints, systems/applications, network-connected equipment, and platforms.

12. Monitoring and Review

12.1. The monitoring and review of this Procedure is based on the objectives outlined in Section 3.0.

12.2. The ITS Department will be responsible for monitoring and reviewing this Procedure to ensure alignment with legislative changes, information technology practices and/or Ministry of Education directives.