Table of Contents

1. Introduction 2
1.1. Purpose 2
1.2. Scope 2
1.3. Responsibilities 2
1.4. General Procedure Definitions 3
2. ICT Asset Usage Procedure 3
2.1. Purpose 3
2.2. Scope 3
2.3. Procedure Definitions 3
3. Access Control Procedure 4
3.1. Purpose 4
3.2. Scope 4
3.3. Procedure Definitions 4
4. Password Control Procedure 4
4.1. Purpose 4
4.2. Scope 4
4.3. Procedure Definitions 5
5. Electronic Communication Procedure 5
5.1. Purpose 5
5.2. Scope 5
5.3. Procedure Definitions 5
6. Internet Procedure 6
6.1. Purpose 6
6.2. Scope 6
6.3. Procedure Definitions 6
7. Antivirus Procedure 7
7.1. Purpose 7
7.2. Scope 7
7.3. Procedure Definitions 7
8. Information Classification Procedure 7
8.1. Purpose 7
8.2. Scope 7
8.3. Procedure Definitions 8
9. Remote Access Procedure 8
9.1. Purpose 8
9.2. Scope 8
9.3. Procedure Definitions 8
10. Outsourcing Procedure 9
10.1. Purpose 9
10.2. Scope 9
10.3. Procedure Definitions 9
11. Annex 9
11.1. Glossary 9

1. INTRODUCTION

The Information Security Procedure identifies all levels of security over the Information and Communication Technology (ICT) department resources to ensure a secure environment.

1.1. Purpose

This Security Procedure document is aimed to define the security requirements for the proper and secure use of the ICT services at the CDSBEO (Catholic District School Board of Eastern Ontario). The goal is to protect the CDSBEO and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation, business and education outcomes.

1.2. Scope

This document applies to all the users in the CDSBEO, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with procedures this document is mandatory for this constituency.

1.3. Responsibilities

Roles	Responsibilities
Chief Information Officer	• Accountable for all aspects of the CDSBEO's information security.
ICT supervisors	• Responsible for the security of the ICT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Procedure documents. • Ensure security communication requirements to all impacted CDSBEO users. • Ensure ICT infrastructure supports Security Procedures. • Respond to information security incidents as outlined in F1:4 Security Incident Management. • Manage disaster recovery plans.
Information Owners	• Information Owners are users with additional security access throughout the CDSBEO. • Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
ICT Team	• Implements and operates ICT security. • Implements the privileges and access rights to the resources. • Supports Security Procedures.
Users	• Follows Security Procedures. • Report any attempted security breaches.

1.4. General Procedure Definitions

a) Exceptions to the procedures defined in any part of this document may only be authorized by the Chief Information Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
b) All the ICT services should be used in compliance with the technical and security requirements defined in the design of the services.
c) Infractions of the procedures in this document may lead to disciplinary actions. In some serious cases they could even lead to prosecution.

2. ICT ASSET USAGE PROCEDURE

2.1. Purpose

The ICT Asset Usage Procedure section defines the requirements for the proper and secure handling of all the ICT assets in the CDSBEO.

2.2. Scope

The procedure applies to computer devices including but not limited to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the ICT services.

2.3. Procedure Definitions

a) ICT assets must only be used relating to the business and school activities they are assigned and/or authorized.
b) All users are responsible for the preservation and correct use of the ICT assets they have been assigned.
c) All the ICT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
d) Active computer devices such as but not limited to desktop and laptops must be secured if left unattended. Whenever possible, this procedure should be automatically enforced.
e) Access to assets is forbidden for non-authorized personnel.
f) All personnel interacting with the ICT assets must have the proper training.
g) Users shall maintain the assets assigned to them clean and free of accidents or improper use.
h) Access to assets at all CDSBEO locations must be restricted and properly authorized, including those accessing remotely. The CDSBEO's portable computing devices such as but not limited to laptops, tablets and other equipment used at external location must be periodically checked and maintained.
i) The ICT Technical Team is responsible for maintaining and upgrading configurations. No other users are authorized to change or upgrade the configuration of the ICT assets. That includes modifying hardware or installing software.
j) Special care must be taken for protecting laptops, tablets and other portable assets from being stolen.
k) When travelling by plane, portable equipment like laptops and tablets must remain in possession of the user as hand luggage.

l) Whenever possible, encryption and erasing technologies should be implemented in portable assets in case of theft.
m) Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the Chief Information Officer.
n) Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically erased and destroyed by an Information and Communication Technology Team member before disposal.

3. ACCESS CONTROL PROCEDURE

3.1. Purpose

The Access Control Procedure section defines the requirements for the proper and secure control of access to ICT services and infrastructure in the CDSBEO.

3.2. Scope

This procedure applies to all the users in the CDSBEO, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

3.3. Procedure Definitions

a) Any system that handles valuable information must be protected with a password-based access control system.
b) Access to resources should be granted on a per-group basis rather than on a per-user basis.
c) Access shall be granted under the principle of "less privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
d) Whenever possible, access should be granted to centrally defined and centrally managed identities.
e) Users should refrain from trying to tamper or evade the access control to gain greater access than they are assigned.
f) User are required to notify ICT immediately in the event their access is greater than required to perform their respective duties.

4. PASSWORD CONTROL PROCEDURE

4.1. Purpose

The Password Control Procedure section defines the requirements for the proper and secure handling of passwords in the CDSBEO.

4.2. Scope

This procedure applies to all the users in the CDSBEO, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

4.3. Procedure Definitions

a) Any system that handles valuable information must be protected with a password-based access control system.
b) Every user must have a separate, private identity for accessing ICT network services.
c) Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
d) Users with access to sensitive data must have a strong, private, alphanumeric password to be able to access any service. Must use three of the follow categories: little case, large case, numeric and special characters.

User	**Passwords**			
	Length	**Age**	**History**	**Complexity**
Generic Student	Minimum 5 char	None	None	None
Generic Staff	Minimum 8 char	180 days	3	True
Elementary students	Minimum 5 char	None	None	None
Secondary students	Minimum 8 char	None	3	True
Staff	Minimum 8 char	180 days	3	True

e) The Administrator account is only accessible by the Associate Chief Information Officer. A sealed envelope with the password is given to the Chief Information Officer immediately after the Administrator password is changed.
f) Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
g) Whenever a password is deemed compromised, it must be changed immediately.
h) Any user account that is exhibiting hacking activities must be locked immediately.

5. ELECTRONIC COMMUNICATION PROCEDURE

5.1. Purpose

The Electronic Communication Procedure section defines the requirements for the proper and secure use of electronic communication in the CDSBEO.

5.2. Scope

This procedure applies to all the users in the CDSBEO, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3. Procedure Definitions

a) All the assigned electronic communication identities such as but not limited to addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the CDSBEO. Occasional use of electronic communication identities on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the CDSBEO system resources and the productivity of the work is not affected.
b) Use of the CDSBEO resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the CDSBEO business is strictly forbidden.

c) In no way may the electronic communication identities be used to reveal confidential or sensitive information from the CDSBEO outside the authorized recipients for this information.
d) Using the electronic communication identities resources of the CDSBEO for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
e) Use of the CDSBEO electronic communication identities resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the CDSBEO, the associated account is automatically deactivated according to established procedures for the lifecycle of the accounts using the identity management system.
f) Users must have separate identities to access their electronic communication identities and individual storage resources, except specific cases in which common usage may be deemed appropriated.
g) Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged.
h) Identities for accessing corporate electronic communication identities must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the CDSBEO's procedures for managing identities. Sharing of passwords is prohibited. Users should not impersonate another user.
i) Attachments must be limited in size according to the specific procedures of the CDSBEO. Whenever possible, links to documents in cloud based and/or shared drives should be encouraged. Restrictions to attachments are automatically enforced.
j) Scanning technologies for virus and malware must be in place on all vulnerable end devices and servers to ensure the maximum protection for incoming and outgoing electronic communications.
k) Security incidents must be reported and handled as soon as possible in accordance with the F1:4 Security Incident Management Procedure. Users should not try to respond by themselves to security attacks.
l) Corporate electronic communication storage content should be centrally stored in locations where the information can be backed up and managed according to the CDSBEO procedures.

6. INTERNET PROCEDURE

6.1. Purpose

The Internet Procedure section defines the requirements for the proper and secure access to Internet.

6.2. Scope

This procedure applies to all the users in the CDSBEO, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

6.3. Procedure Definitions

a) All Internet access must be limited and filtered for all users.
b) Internet access is primarily for business and educational purpose. Some limited personal navigation is permitted if in doing so there is no perceptible consumption of the CDSBEO system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
c) Inbound and outbound traffic is regulated using firewalls on the perimeter.

d) In accessing Internet, users must behave in a way compatible with the values of the CDSBEO. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
e) Internet traffic is monitored at firewalls. Any attack or abuse should be promptly reported in accordance with the F1:4 Security Incident Management Procedure.
f) Reasonable measures must be in place at servers, end devices and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

7. ANTIVIRUS PROCEDURE

7.1. Purpose

The Antivirus Procedure section defines the requirements for the proper implementation of antivirus and other forms of protection in the CDSBEO.

7.2. Scope

This procedure applies to servers, end devices and equipment in the CDSBEO, including portable devices like laptops and tablets that may travel outside of the CDSBEO facilities. Some procedures apply to external computers and devices accessing the resources of the CDSBEO.

7.3. Procedure Definitions

a) All vulnerable computers and end devices with access to the CDSBEO network must have an antivirus client installed, with real-time protection.
b) All servers and workstations owned by the CDSBEO or permanently in use in the CDSBEO facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to the CDSBEO network or that can be managed via secure channels through Internet.
c) All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
d) Guest computers and all computers that connect to the CDSBEO's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

8. INFORMATION CLASSIFICATION PROCEDURE

8.1. Purpose

The Information Classification Procedure section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the CDSBEO information.

8.2. Scope

This procedure applies to all the information created, owned or managed by the CDSBEO, including those stored in electronic or magnetic forms and those printed in paper.

8.3. Procedure Definitions

a) Information owners must ensure the security of their information and the systems that support it.
b) ICT is responsible for ensuring the confidentiality, integrity and availability of the CDSBEO's assets, information, data and ICT services.
c) Any breach must be reported immediately in accordance with the F1:4 Security Incident Management Procedure. If needed, the appropriate countermeasures must be activated to assess and control damages.
d) Information in the CDSBEO is classified according to its security impact. The current categories are: confidential, sensitive, shareable, public and private.
e) Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Chief Information Officer.
f) Information defined as sensitive can be handled by a greater number of persons. If sensitive data is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.
g) Information defined as shareable can be shared outside of the limits of the CDSBEO, for those clients, CDSBEOs, regulators, etc. who acquire or should get access to it.
h) Information defined as public can be shared as public records, e.g. content published in the company's public Web Site.
i) Information deemed as private belongs to individuals who are responsible for the maintenance and backup.
j) Information is classified jointly by the Chief Information Officer and the Information Owner.

9. REMOTE ACCESS PROCEDURE

9.1. Purpose

The Remote Access Procedure section defines the requirements for the secure remote access to the CDSBEO's internal resources.

9.2. Scope

This procedure applies to the users and devices that need access the CDSBEO's internal resources from remote locations.

9.3. Procedure Definitions

a) To gaining access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
b) Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
c) Remote access to confidential information should not be allowed. Exception to this rule may only be authorized in cases where is strictly needed.
d) Users must not connect from public computers unless the access is for viewing public content.

10. OUTSOURCING PROCEDURE

10.1. Purpose

The Outsourcing Procedure section defines the requirements needed to minimize the risks associated with the outsourcing of ICT services, functions and processes.

10.2. Scope

This procedure applies to the CDSBEO; the services providers to whom ICT services, functions or processes are been outsourced, and the outsourcing process itself.

10.3. Procedure Definitions

a) Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
b) Whenever possible, Broader Public Sector Purchasing Guidelines should be followed to select between several service providers.
c) In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
d) A service contract and defined service levels must be agreed between the CDSBEO and the service provider.
e) The service provider must get authorization from the CDSBEO if it intends to hire a third party to support the outsourced service, function or process.

11. ANNEX

11.1. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of ICT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An ICT service provider that is part of a different CDSBEO from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Procedure	The procedure that governs the CDSBEO's approach to information security management
Outsourcing	Using an external service provider to manage ICT services.
Procedure	Formally documented management expectations and intentions. Procedures are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, ICT infrastructure etc.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.

Table 1. Glossary.