Sheridan	THE SHERIDAN COLLEGE INSTITUTE OF TECHNOLOGY AND ADVANCED LEARNING

Title: Information Security Policy

Original Date: November 13, 2024 **Date of Approval:** November 13, 2024	**Effective Date:** November 13, 2024 **Last Review Date:** November 13, 2024	**Approved By:** ☐ Board of Governors ☒ President & Vice Presidents

1. Purpose

The Information Security Policy ("Policy") establishes a framework to protect the confidentiality, integrity, and availability of Sheridan College Institute of Technology and Advanced Learning's ("Sheridan") Information Technology ("IT") Resources. It aims to provide secure services to our community while ensuring compliance with applicable legal and regulatory requirements.

This Policy outlines the shared responsibility of Sheridan community members to use Sheridan IT Resources in a manner that preserves the secure use of these resources and safeguards against unauthorized access, disclosure, alteration, and destruction of data. This Policy also establishes the leadership responsibilities of IT and the IT Security department regarding information security.

2. Scope

This Policy applies to all Sheridan employees, students, alumni, contractors, and other individuals using Sheridan IT Resources. The requirements set out in this Policy are applicable to the use of all data, systems, electronic and computing devices, and services owned and/or managed by Sheridan.

3. Definitions

"Access" refers to access to systems, services and information that is accessible through such services.

"**Account**" refers to an identity created for an individual in a computer or computing system, consisting of a unique username and password. This identity allows the individual to log in to Access Sheridan IT Resources.

"**Account Holder**" or "**Individual**" is the individual for whom the Account was provisioned, and the individual who uses or is responsible for the Account.

"**CASL**" means Canada's Anti-Spam Legislation.

"Commercial Electronic Message" means an electronic message that, considering the content of the message, any hyperlinks to content on a website or other database, or the contact information within the message, could reasonably be concluded to have, as its purpose or one of

its purposes, the encouragement of participation in a commercial activity.

"Information Technology (IT)" refers to Sheridan's Information Technology (IT) Department.

"**Information Technology (IT) Resources**" includes all Sheridan owned or managed hardware and software assets, including computers, communication networks, systems / applications and cloud-based solutions.

4. Policy

Sheridan will act appropriately to preserve the confidentiality, integrity, and availability of information and related hardware and software assets to maintain a secure information technology environment. Sheridan provides a safe and secure environment for the collection, storage, Access, processing, retrieval and removal of information.

Information security is a collective responsibility, led by IT, where each member of the Sheridan community plays a crucial role in safeguarding Sheridan IT Resources. Sheridan prioritizes building a strong security foundation by implementing cyber security best practices, educating the community about common threats, and ensuring systems are regularly updated. Sheridan acts proactively with a focus on prevention through vigilant monitoring and response. Resources are allocated in a manner which prioritizes the protection of critical information and technological assets in accordance with industry leading practices. See section 7 on 'Related Documents' for specificity.

4.1. Account and Password Management

- Accounts may only be accessed by the Individual to whom the Account was assigned unless otherwise stated in Sheridan's Acceptable Use Policy and subject to appropriate approvals.
- Account Holders must log out or lock Access to an IT Resource when leaving it unattended.
- All Accounts are protected by a password. Account passwords must never be shared.
- Passwords should be changed under the following circumstances:
    - the first time the Account is accessed with the initial temporary password and within 24 hours; or
    - when there is any concern on the part of the Account Holder about the security of the Account / password (e.g., a suspected compromise); or
    - when requested to do so by Sheridan IT; or
    - when prompted by the system.
- Passwords must meet the complexity requirements as outlined in the Password Management Procedure, wherever technically possible.
- As per a leading industry standard for identity management, passwords that have multi factor authentication (MFA) enabled, do not need to be changed unless they have been linked to a breach / suspected compromise.
- MFA must be enabled for all Accounts to provide an additional layer of security, wherever possible.

4.2. Cyber Hygiene Practices

- Individuals should review cyber awareness alerts shared in institutional communication channels (e.g., Sheridan Insider, Sheridan Weekly, email) to remain aware of security best practices, recent policies published, controls implemented, threat advisories, and other relevant information related to information security.
- Account Holders must promptly report any instances of misuse, suspicious activity, or unauthorized access involving Sheridan IT Resources to IT using the channels provided below.

Individuals should also contact IT immediately if they suspect their device may be infected.

  - Service Sheridan (or)
  - Phone: 905-845-9430 ext. 2150 (or)
  - Support Chat

- If Individuals suspect that their Account has been compromised, they should reset their passwords immediately at the 'Sign in' prompt. They should also notify IT as noted above.
- Individuals should not open message attachments or click on hyperlinks from unknown sources. If an Individual is doubtful about the legitimacy of an email, they should identify it to IT by clicking on the 'Report phishing' button in Microsoft Outlook (Sheridan's email platform). For more information, click here.
- Account Holders must use Sheridan IT provided Virtual Private Network software to Access systems while working remotely, in cases where secure Access is warranted (e.g., server / database administration).
- Confidential information should be protected and handled appropriately (e.g., tagging as sensitive and / or encrypted using appropriate mechanisms)

4.3. Incident Management and Reporting Obligations

Sheridan has an all-hazards Emergency Management Plan with an annex dedicated to cyber incidents. All incidents are managed using six steps in alignment with a leading industry framework.

(a) Preparation – the necessary preparations to allow us to identify and handle incidents
(b) Identification - the initial detection, reporting and identification of an incident
(c) Containment - preventing the spread of the incident in the short term
(d) Remediation - removing the threat and starting the work to repair the damage / prevent similar attacks in the future
(e) Recovery - getting things up and running again / restoring normal operations
(f) Post incident activities – completing a review of the incident and lessons learned to improve the incident response process

Incidents are classified under three severity levels as (a) normal operations (b) minor incident (c) major incident with specific actions and teams that will be assembled to manage the incident.

Sheridan also has reporting obligations externally depending on the type and severity of the incident (e.g., to the Ministry of Colleges and Universities and the Information and Privacy Commissioner of Ontario in case of breach of personal data as governed by the *Freedom of Information & Protection of Privacy Act* and the *Personal Health Information Protection Act*, local authorities / law enforcement, as appropriate.

In addition, Sheridan shares information related to incidents and any lessons learned with the Canadian Centre for Cyber Security, Canadian Shared Security Operations Centre and other post-secondary institutions, as appropriate.

5. Roles and Responsibilities

5.1 IT Security

The IT Security department is responsible for ensuring appropriate security measures / safeguards are in place to protect Sheridan IT Resources from vulnerabilities and potential threats by working collaboratively with other departments as follows:

- Establishing an IT security program that aligns with Sheridan's strategy and objectives.
- Establishing cyber related policies, standards, best practices / procedures, and controls.
- Raising awareness on information security topics such as prevalent industry threats and cyber safe practices / suggestions, to foster security conscious behaviour, reflecting Sheridan's commitment to providing a secure and resilient digital environment.
- Monitoring the IT environment for any suspicious activity and undertaking containment, mitigation, and remediation actions as appropriate. This extends to managing incidents by working with the other departments, as appropriate.
- Responding to internal / external audits and support compliance related requests – both internal (e.g., academic integrity issues) and external (e.g., legal requests and investigations).
- Providing consultative / advisory services by reviewing new applications, feature enhancements, and integrations to existing systems / tools. This includes reviewing IT related third parties pre-contracting for security and privacy provisions.

5.2 Director IT Security

The Director, IT Security is responsible for:

- Developing and maintaining policies designed to protect Sheridan IT Resources.
- Establishing and maintaining high-level standards and related procedures for Sheridan's information and systems.
- Selecting, implementing, and administering controls and procedures to manage information security risks.
- Receiving reports of incidents and threats that may have an impact on Sheridan IT Resources.
- Ensuring that all reported security breaches are fully investigated, and the appropriate remedial action is taken.
- Acting as Sheridan's representative to external bodies on matters relating to IT security.
- Providing information security advice to all levels of the Sheridan community.

5.3 Managers

Managers are responsible for:

- Determining and arranging for their employees' specific system Access and only IT Resources essential for their designated tasks.
- Ensuring their employees are familiar with policies and procedures regarding the appropriate use of Sheridan IT Resources.
- Reporting instances of suspected misuse or unacceptable use of Sheridan IT Resources by a Sheridan employee, contractor, volunteer, co-op student, student worker, visitor, or other person for whom they are responsible to Human Resources and system security concerns/vulnerabilities to IT as set out in *section 4.2.*
- Ensuring that system Access is removed when an Individual leaves Sheridan or their responsibilities change.

5.4 Employees

Employees are responsible for protecting Sheridan's systems and networks. Employees are responsible for reporting instances of suspected misuse or unacceptable use of Sheridan IT Resources by a Sheridan student to the Office of Student Rights and Responsibilities, Student Affairs, and system security concerns/vulnerabilities to IT as set out in *section 4.2*

6. Policy Compliance

Exceptions to this Policy will not be approved unless there is a legitimate business reason to do so. If such a situation arises (i.e., to continue business operations or to support a legal request / investigation), exceptions will be granted by the relevant Vice President, as appropriate.

Sheridan may take appropriate disciplinary measures in cases of attempted violation of this Policy, regardless of the attempt's success or failure.

Any attempt to circumvent local, provincial, federal or international laws through Sheridan IT Resources may result in litigation against the offender by the appropriate authorities.

Please direct any questions related to this Policy to itsecurity@sheridancollege.ca

The Responsible Executive for this policy shall be the AVP & Chief Information Officer, Information Technology as delegated by the VP, Administrative Services.

7. Related Documents

Acceptable Use Policy

Sheridan's Encryption Standard

NIST Cybersecurity Framework (CSF) 2.0

Payment Card Industry Data Security Standard (PCI DSS)

NIST Digital Identity Guidelines

Cyber Incident Response Framework

Sheridan's Emergency Management Plan - Cyber

Password Management Procedure

Privacy Policy

Employee Technology Policy

Records and Information Management Policy

Free Speech Policy

Social Media Policy

CASL Explanatory Slide Deck

Employees CASL Checklist

CASL (Canada's Anti-Spam Legislation) Q & A