DALHOUSIE UNIVERSITY **Information Security Policy**	*Policy Sponsor:* Assistant Vice-President, Information Technology Services	*Approval Date:* **November 26, 2024**
	Responsible Unit: Information Security Office	*Amendments:*

A. Background & Purpose:

Dalhousie University (hereinafter referred to as “the University”) has legal and ethical obligations to protect the confidentiality, integrity, and availability of information managed by the institution, and information contained within University information systems. The University is committed to promoting a culture of information management which enables the protection of personal and institutional information and continuous improvement of information security practices.

The purpose of this policy is to:

i. Establish a set of information management and security standards that supports the development of systems and processes which protect confidentiality, integrity, and availability of information held or managed by the institution.

ii. Ensure that the University complies with all applicable information security related legislative obligations, governance requirements, and contractual obligations governing information in its custody or control.

iii. Ensure that all members of the University Community understand their responsibilities and are accountable for protecting information and respecting information confidentiality, integrity, and availability standards when carrying out their duties.

B. Definitions:

Terms used in this policy are defined in Appendix “A” of this document.

C. Application:

i. This policy applies to:

a. All members of the University Community - persons who are directly, or indirectly, affiliated with Dalhousie University. For example:

i. Employees of the university (e.g. - faculty and operational staff: full-time, part-time and temporary);

ii. Students and alumni;

iii. All entities or organizations using the Dalhousie network, software applications or computing resources.

iv. Service providers contracted to handle information in the custody and control of the University;

v. Volunteers, including Dalhousie’s Board of Governors;

b. All information under the custody or control of the University:
   i. in all recorded formats, digital or paper and in all storage locations;
   ii. related to staff, faculty, students, alumni, clients, members of the public, and other individuals involved in University operations and activities;
   iii. including institutional information: academic, research, and operational.

ii. Specific interpretation of principles and requirements defined in this policy shall be made by the Information Security Office, and executed through the Office of the CIO as a series of protocols, guidelines, and standards published through Information Technology Services (ITS). Protocols, guidelines, and standards will be updated annually. Where interpretation is required, preference will be given to standards or implementations consistent with current NIST Cybersecurity Framework guidance.

iii. Enforcement of requirements shall come from the Office of the CIO. Where information management practices do not meet the requirements of this policy, either an exception to policy must be granted by the Office of the CIO (with appropriate risk mitigations in place), or affected services, accounts or devices will be removed from University networks and services until they can be brought into compliance with this policy.

The Office of the CIO, through the Information Security Office, will work with University groups to bring them into compliance with this policy, or document granted exceptions and appropriate risk mitigations for a non-compliant information management process.

D. Policy:

i. University Policy Compliance (general) – the following University policies must be followed in order to remain in compliance with this Information Security Policy. Violations of standards within these policies are considered a violation of the Information Security Policy.
   a. Acceptable Use Policy (AUP)
   b. Privacy Policy
   c. Data Administration Policy
   d. Records Management Policy
   e. Payment Card Processing Policy

ii. Legal Compliance

   a. The University has legal responsibilities to properly manage information in its custody. Examples of legal requirements are inclusive of, but not limited to:
      i. Legislative obligations (e.g.):
         1. Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) legislation
         2. Nova Scotia's Personal Information International Disclosure Protection Act (PIIDPA) legislation
      ii. Governance obligations (e.g.):
         1. The Payment Card Industry Data Security Standard (PCI DSS)

2. Regulated research information and equipment (e.g.):
    a. U.S. National Institutes of Health (NIH) controlled access data sets
    b. Canadian National Security Guidelines for Research Partnerships

iii. Contractual obligations

b. University services and units which manage legal and regulated information must protect and manage that information in accordance with the appropriate standard.

c. University services not in legal compliance with these information standards are in violation of the University's Information Security Policy.

iii. Information Security Incident Management

a. Reporting

i. Information security incidents should be reported as soon as observed, and must be reported no later than 24 hours after observation.

ii. Information and cyber security events which have an impact, or the potential to have an impact, on University operations or information management obligations must be reported to ITS for triage, risk assessment, and incident management.

iii. If an information event puts personal, confidential, or sensitive information at risk, the Privacy Office must also be notified of the incident.

iv. Reported incidents should be sent through standard communications channels and escalation procedures to ITS. A time-sensitive medium (phone call, live chat, in-person, etc.) must be used for incident reporting.

b. Incident Management Process

i. Information security incidents will follow the published *Incident Management Process* and associated incident playbooks managed by ITS.

iv. Information Security Training & Education

a. All individuals with access to a University directory account must complete regular training in information management, privacy, and security standards, appropriate for their access privileges.

b. Current requirements for training can be found in the University *Information Management Training Standard*.

v. Data and Information Management

a. Minimization

i. Data use should be limited in collection, storage, and processing of personal information to only what is strictly necessary for identified purposes within the University.

b. Classification Standard

i. All information in the University's custody and control must be classified by the units collecting or managing the information into classifications provided in the University *Information Security Classification Standard*.

ii. Information must be stored in University services and locations appropriate to the information classification, as listed in the *Information Security Classification Standard*. Storage of University information outside of guidelines established by the standard is a violation of the University's Information Security Policy.

iii. Exceptions to the *Information Security Classification Standard* must be approved and registered with the Office of the CIO.

c. Encryption

i. All services and devices processing or storing information classifications other than "Public" (hereinafter referred to as "non-public University information") must have their storage areas encrypted using the current University *Encryption Standard*. This requirement encompasses servers, workstations, mobile devices, service storage arrays, and includes cloud and contracted IT storage locations.

ii. Personal devices which store or cache non-public University information, beyond that user's personal information, must use device storage encryption as a condition for accessing University services and/or storing non-public University information.

d. Disposal

i. Information storage resources containing non-public University information must be securely destroyed or wiped when no longer retained or commissioned, in accordance with the University *Secure Hardware Disposal Procedure*.

vi. Device Management

a. Patch Management

i. Device operating system security patches and service/application software updates must be installed in a timely manner, in accordance with the University *Minimum Standard for Networked Devices*.

ii. Devices not in compliance with minimum standards must either remain disconnected from University networks and services until updated, or an exception granted and documented, with appropriate risk mitigations, through the Office of the CIO.

b. Virus and Malicious Software (malware) Prevention

i. All devices operating on University networks, interacting with University services, or storing non-public University information must have virus and malware prevention installed, and up-to-date, if the device supports such protections.

ii. University-managed devices must have University-provided virus and malware protection software installed and up-to-date, if it is provided for that device type.

iii. The University reserves the right to refuse services and access to any device not operating with virus and malware prevention installed.

c. Software Installation and Vulnerabilities

i. Software on University-managed devices will be standardized based on University needs for device and service use. Exceptions to standards will be granted based on the work requirements of the individual user.

ii. All software installed on University-managed devices will be evaluated and monitored for security risks and vulnerabilities, as well as inappropriate device activity, on a regular basis. Devices with potentially malicious software will be isolated from the network while an investigation is conducted.

iii. Software on any device identified as creating a risk to the University, its constituents, or University-managed information may be banned from University networks, devices, and services.

d. Internet of Things

i. Specialized computing devices, AKA “Internet of Things” (IoT) devices, when connected to a University network, must wherever possible operate in isolated, protected environments. These devices should not have general access or visibility to the Internet, or to University networks they do not need to access.

ii. Examples of IoT devices include: alarm systems, cameras, building environment control systems, power management systems, wearable and medical devices, etc.

iii. Exceptions to IoT devices policy must be granted by and documented with the Office of the CIO.

vii. Information Sharing and Requests

a. Research Information Hosting

i. Research information hosted at the University, when it has contractual, governance, oversight, or privacy protection obligations, must have a research information security plan created and filed with the Office of Research Services (ORS). These plans must be filed with ORS before signing or accepting research information hosting agreements.

ii. Templates for use with common research information security plans are available as reference guides through the Office of Research Services.

b. Contracts: Information Extraction/Equipment Return Policy

i. Contracts for hosting of information in the custody and control of the University must include reasonable provisions to extract or destroy University information at the end of the contract period, as part of contracted services.

ii. Leased equipment, or equipment returned to an external partner, containing non-public University managed information must be securely wiped in compliance with the University *Secure Hardware Disposal Procedure*.

viii. Internet and Network Access Security

a. Minimum Standards for Networked Devices

i. All University IT resources and all devices, independent of their location or ownership, when connected to a University network, or when storing, processing, or accessing institutional information hosted at any location, must comply with the University's published *Minimum Standards for Networked Devices*.

ii. Devices that do not meet these standards may be disconnected from University networks and/or hosted services without prior warning.

iii. Devices with access to internal, confidential or sensitive information may have additional requirements placed on them for access to University services. Those additional requirements may be defined by a service or resource's data security protection plan, or by University standards for accessing information in specified information classifications.

iv. For the purposes of this standard, guest networks on University campuses are not considered a University network.

b. Firewall and Intrusion Prevention

i. Firewalls on University network perimeters must have a deny-by-default and allow-by-exception configuration for inbound connections.

ii. Firewalls on central infrastructure and data center resources must have a deny-by-default and allow-by-exception configuration for both inbound and outbound connections. Service delivery requirements will determine acceptable firewall exceptions.

iii. Network attached systems must, wherever possible, utilize host-based firewalls and access control lists (ACLs). These controls must be enabled and configured to block all inbound traffic that is not explicitly required for the intended use of the device. Use of a network-based firewall does not obviate the need for host-based firewalls.

iv. Intrusion prevention and detection systems, and network access standards, will be managed by and/or published through ITS.

v. All University network devices and device activity may be reviewed by intrusion prevention and detection systems, and Security Operations staff, as a requirement for using the network and accessing services.

c. Vulnerability Scanning and Penetration Testing

i. Vulnerability scanning and penetration testing is allowed on all devices connecting to a University network, as a condition of use for the network.

ii. Vulnerability scanning will be conducted regularly on University network devices, and results must be acted upon by device and service owners in a timely manner. Patching and mitigation schedules will follow the minimum standards required within this policy, as a condition of use for the network.

d. VPN standards

   i. All use of VPN tools to access University networks must follow the University's published VPN connectivity requirements and use standards provided in the University *VPN protocol*.

ix. Auditing

a. Auditing of the confidentiality, integrity, and availability of information resources is a necessary requirement to control information security risks. The University reserves the right to audit any physical or digital information resource under the authority and/or management of the institution. This includes any account, device, service, network, or physical environment which contains or has access to information resources of the University.

b. Privacy of individuals will be respected when audits are conducted, and audits will conform with the Privacy Policy of the University.

x. Authentication and Authorization

a. Authentication

   i. Authentication measures and methods must be implemented commensurate with the risk to information stored on a device or service, and the risk of service or device misuse.

   ii. The University's *Authentication and Passwords Standard* must be followed on all University services and devices which store or access non-public University information.

b. Access Control and Elevated Privileges

   i. Access to all information resources, data repositories, and services must be managed using the Principle of Least Privilege:

      1. *"Each entity in an information management system is granted the minimum system authorizations and resources that the entity needs to perform its function."* [1]

   ii. Accounts which access non-public University information must have authorization given (specifically, in-principle, or via a workflow process) to access non-public information for a specific identified purpose.

   iii. Accounts which no longer have a specific identified purpose requiring access to non-public University information must have their access removed in a timely manner. Current definitions for managing access control timelines can be found in the University *Access Control Standard*.

   iv. Devices and services storing non-public University information must re-lock themselves or require re-authentication after a short time period of disuse. Current definitions for device locking and re-authentication requirements can be found in the University *Access Control Standard*.

[1] NIST online glossary, NIST SP 800-171 rev 2.

v. Individuals responsible for issuing elevated privileges on University information must regularly review, for roles with an elevated privilege, access permissions and activity. Reviews will be based on access control review guidelines found in the University *Access Control Standard*.

xi. Service Management Security

a. Service Development & Lifecycle

i. All general-use IT services at the University should have a service development and lifecycle plan created and documented before the service is put into production.

ii. Service development and lifecycle plans should refer to the University *Service Development Plan Standard* for guidance.

iii. All general-use IT services at the University should have changes administered through the University's *Change Management Process*.

iv. All University-provided services must have a *Privacy Impact Assessment* (PIA) conducted through the Privacy Office. This requirement applies to any new services, or if an existing service materially changes.

b. Physical Access, Environmental Controls

i. All general-use IT services at the University must be housed in official data centre locations designated by the University for IT services, or in approved cloud hosting environments. Physical access, environmental controls, and security controls for such services, to ensure information and service confidentiality, integrity, and availability, are defined in the University *Data Centre Standard*.

ii. Exceptions for general use IT service infrastructure hosting must be granted by and documented with the Office of the CIO.

c. Third Party Service Providers and Sub-Contractors

i. Third party service providers conducting work on, or providing support for, general-use IT services should be provided "escorted access" for their work on University IT services, whether it is on site or remote work.

ii. Third party provider accounts with access to University IT services should be disabled when not required for active work.

iii. Sub-contractors, where they work for or with third parties, are required to follow all University policies and procedures applicable to their work.

xii. Backup and Recovery Standards

a. Scope

i. University information services considered critical to the work of the institution must be defined in the University *IT Services Business Continuity Plan*.[2]

[2] This is a forthcoming plan slated to start development in 2025.

b. Backup

   i. All critical University information services and information resources must have regular backups conducted, appropriately scoped in frequency and retention to the impact to the University if the information were lost due to device destruction, data corruption, or disaster.

   ii. Backup of University information must be offline and remote from the original data resource or service, or separated from the network on a cloud service designed for this purpose.

   iii. All backup data must be encrypted, with offline backup of encryption keys.

   iv. All backup data must be secured behind authentication credentials which are separated from standard university authentication systems.

c. Recovery

   i. Recovery processes for critical University information services must be documented and reviewed annually.

   ii. Recovery procedures for critical University information services should be tested, or a "tabletop exercise" conducted to walk through recovery procedures, annually. Selecting an example service from related services to walk through recovery procedures is sufficient to meet this requirement.

   iii. Recovery procedures on backup data for critical University information services must be tested quarterly.

xiii. Development Standards for IT Applications

a. Specific standards, toolsets, and methods for development work conducted at the University can be found in the University *Developer Standard* and must be referenced for all general-use IT applications and services at the University where development work is performed.

Associated Protocols and Standards:

A. Information Security Classification Standard
B. Incident Management Process
C. PCI Compliance Protocols
D. VPN Protocol
E. Encryption Standard
F. Minimum Standards for Networked Devices
G. Information Management Training Standard
H. Access Control Standard
I. Service Development Plan Standard
J. Change Management Process
K. Data Centre Standard
L. Secure Hardware Disposal Procedure
M. IT Services Business Continuity Plan
N. Developer Standard
O. Exception to Policy Protocol

Appendix A: Definitions

Data - Representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. Distinct pieces of digital information that have been formatted in a specific way.

Entities / Organizations – affiliated businesses, research groups, and partners who make use of Dalhousie networks and services, but are not officially part of the University

Escorted access – the practice of a University employee providing access to a 3rd party technician or support resource, while actively monitoring the activities the 3rd party employee conducts

General-use IT services - Enterprise information systems, digital platforms and services used across the University, large information systems used in multiple departments, and information systems used by many individual University Community members.

Information - Data which is processed, organized, structured or presented in a given context so as to make it useful. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Non-public University information – Information which has been identified as any information classification other than "Public" according to the University's Information Classification Standard.

Personal, confidential, or sensitive information:

> **Personal** – Information about an identifiable individual (e.g. – names, addresses, personal health information, government identifiers, financial account information)
>
> **Confidential** - Business or personal information which is intended for a very specific use. It cannot be disclosed except to those who need to know the information by virtue of their role at the University, and can only be used for specific authorized purposes.
>
> **Sensitive** – Information for which there exists a regulatory or contractual obligation to manage the information in a specified manner exceeding other classification standards.

Tabletop exercise – The practice of walking through an operational process or procedure in a group without actually taking the direct actions specified by the process. This is often conducted around a table (thus "tabletop") by a group wishing to test or ensure that the process is sound, and they have identified all of the process elements.

University – Dalhousie University

University Community - all persons who are directly, or indirectly, affiliated with Dalhousie University. For example:

i. Employees of the university: faculty and operational staff (full-time, part-time and temporary);
ii. Students and alumni;
iii. All entities or organizations using the Dalhousie network, software applications or computing resources.
iv. Service providers contracted to handle information in the custody and control of the University; Volunteers, including Dalhousie's Board of Governors;