DALHOUSIE UNIVERSITY **Acceptable Use Policy**	*Policy Sponsor:* Vice-President Finance and Administration	*Approval Date:* **November 26, 2024**
	Responsible Unit: Information Technology Services	*Amendments:*

1. Background & Purpose

Information and Communication resources are continuously developing and are critical to the operations of the University. However, they can also be used in ways that do not further the University’s mission or advance its core values. Dalhousie is committed to protecting those who use its network and services from illegal or damaging actions by individuals either knowingly or unknowingly.

The purpose of this policy is to define the responsibilities of members of the University Community with respect to the acceptable use of University Information Technology Resources and outline the potential consequences to violation of this policy.

Effective security is a team effort involving the participation and support of every student, staff, faculty member and affiliate who deals with information and/or information systems. It is the responsibility of every community member to know these guidelines, and to conduct their activities accordingly.

2. Application

The policy applies to all equipment that operates on Dalhousie’s computer network and all members of the University Community, hereinafter referred as a “User”, who:

2.1 Access Information under the responsibility of Dalhousie University as students, employees, contractors, consultants, temporaries, and other workers at Dalhousie including all personnel affiliated with third parties or

2.2 Use Information Technology resources (e.g. devices, network) owned, leased, controlled and/or operated by Dalhousie University

2.3 Fall within the control and responsibility of Dalhousie University (e.g. internal networks and systems) or

2.4 Connect and interact with IT resources outside of the control and responsibility of Dalhousie University (e.g. internet, personal IT resources, partner networks/systems)

3. Definitions

In this Policy:

3.1 “Information Technology Resources” refers to all University networks, information systems, communication and collaborations tools, and technology support services.

3.2 “University Community” refers to all persons who are directly or indirectly affiliated with Dalhousie. For example: students, faculty, alumni, staff (full-time and contractors), guests.

3.3 “User” refers to any member of the University Community who has any level of access to Dalhousie’s Information Technology Resources.

3.4 “Proprietary Information” is any University information classified as Internal, Confidential or Sensitive as per the Information Security Classification Standard.

4. Policy

4.1 General Use and Ownership

4.1.1 Dalhousie proprietary information stored on electronic and computing devices whether owned or leased by Dalhousie, the employee or a third party, remains the sole property of Dalhousie. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Electronic Information Storage Guidelines* and the *Information Security Classification Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Dalhousie proprietary information.

4.1.3 You may access, use or share Dalhousie proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees and departments are responsible for exercising good judgment regarding the reasonableness of personal use of technology. Employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Dalhousie may monitor equipment, systems, and network traffic at any time.

4.1.6 Dalhousie reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1.7 Students, staff, and faculty must complete regular training in privacy and security standards, as specified in Dalhousie’s *Information Management Training Standard*. This training will normally be a condition to use the NetID for the year.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Standard for Networked Devices*.

4.2.2 System level and user level passwords must comply with the *Authentication and Password Standard*. Providing access to another individual due to not following this standard, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 20 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 When using a Dalhousie email address outside of official business the user must ensure its use does not imply endorsement by Dalhousie.

4.2.5 All users must use extreme caution when opening email attachments or clicking on links received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user at Dalhousie authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing Dalhousie-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.3.1.1 Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Dalhousie.

4.3.1.2 Unauthorized reproduction and distribution of copyrighted material, including, but not limited to, music, software, or digitizing content from print materials, such as books or magazines, is prohibited unless the reproduction adheres to the principles of fair dealing as outlined by Canadian copyright law and Dalhousie's Fair Dealing guidelines or an active license is held by Dalhousie or the end user for these purposes.

4.3.1.3 Accessing Dalhousie data, servers, services, or accounts for any purpose other than conducting Dalhousie business, even if you have authorized access, is prohibited.

4.3.1.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.1.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).

4.3.1.6 Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.1.7 Using a Dalhousie computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.3.1.8 Making fraudulent offers of products, items, or services originating from any Dalhousie account.

4.3.1.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.3.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.

4.3.1.11 Port scanning or security scanning is expressly prohibited without prior approval of the Infosec Team.

4.3.1.12 Executing any form of network monitoring which will intercept data not intended for the user's device or host, unless this activity is a part of an employee's normal job/duty.

4.3.1.13 Circumventing user authentication or security of any host, network, or account.

4.3.1.14 Introducing honeypots, honeynets, or similar technology on the Dalhousie network.

4.3.1.15 Interfering with or denying service to any other user (for example, denial of service attack).

4.3.1.16 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.17 Providing information about, or lists of, members of the University Community to parties outside Dalhousie, without the explicit permission of those individuals or designated authorities within Dalhousie University.

4.3.1.18 Using Dalhousie network or systems for business activities not specifically authorized by Dalhousie.

4.3.2 Email and Communication Activities

When using University resources to access and use the Internet, users must realize they represent the University. The following behavior is not acceptable:

4.3.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2 Any form of harassment via email, telephone, text, or other means, whether through language, frequency, or size of messages.

4.3.2.3 Unauthorized use, or forging, of email header information.

4.3.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.3.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6 Use of unsolicited email originating from within Dalhousie's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Dalhousie or connected via Dalhousie's network.

4.3.2.7 Posting the same or similar non-business-related messages to large numbers of discussion groups (discussion group spam).

4.3.3 Blogging and Social Media

4.3.3.1. Blogging or posting to social media platforms by employees, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Dalhousie’s systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Dalhousie’s policy, and does not interfere with an employee's regular work duties. Blogging or other online posting from Dalhousie’s systems is also subject to monitoring.

4.3.3.2. Dalhousie’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any University proprietary information, trade secrets or any other material covered by the University’s Information Security Classification Standard when engaged in blogging other than classified “Public”.

4.3.3.3. Employees may also not attribute personal statements, opinions or beliefs to Dalhousie when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Dalhousie. Employees assume any and all risk associated with blogging.

4.3.3.4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Dalhousie’s trademarks, logos and any other Dalhousie intellectual property may also not be used in connection with any blogging or social media activity.

4.4 Consequence of Unacceptable Use

If there is reason to suspect that a User has violated this policy, the Assistant Vice-President, Information Technology Services or the Information Security Office may temporarily revoke, or restrict User Account access privileges of any User, pending further investigation by the Information Security Office.

If the investigation concludes that a violation of this policy has occurred, the Assistant Vice-President, Information Technology Services or the Information Security Office may restrict, suspend or revoke the User’s access to any or all the University’s IT Resources, and the University may:

1. In the case of students, initiate proceedings under the Code of Student Conduct; or
2. In the case of employees, refer the matter for consideration of discipline in accordance with applicable collective agreements, human resource policies, or research contracts, as appropriate, or
3. In the case of community members, restrict access to any/all Dalhousie resources, or
4. Refer the matter to the Dalhousie Legal Counsel Office or Privacy Office.

5 Administrative Structure

The Assistant Vice-President, Information Technology Services is responsible to record, and authorize the investigation of incidents of policy violation reported by the University Community or identified through system administrative activity.

To aid in the investigation of a suspected violation of this policy, the Information Security Office may examine a User's Account information, including, but not limited to, emails, files, and any other material or data connected with the User Account, provided they obtain the Assistant Vice-President, Information Technology Services' prior written approval.

If the investigation concludes that a violation of this policy has occurred, the Academic Head, Research Services, Department Head, Human Resources, Legal Counsel, and/or Privacy Office may be engaged as appropriate in the Non-Compliance Procedure.

6 Related Standards, Procedures and Processes

6.1 Information Security Policy
6.2 Data Administration Policy
6.3 Disclosure of Information Policy
6.4 Guest Access Policy
6.5 Mobile Device Policy
6.6 Networking Extension Policy
6.7 Passwords Policy
6.8 Dalhousie Personal Harassment Policy
6.9 Dalhousie Sexual Harassment Policy
6.10 Statement of Prohibited Discrimination
6.11 Code of Student Conduct
6.12 Ethical Conduct Policy
6.13 Scholarly Misconduct Policy
6.14 Fair Dealing Policy

ITS will publish additional information in the form of IT Protocols and Guidelines. This amplifying information is available on the Information Technology Services internal website at https://dalu.sharepoint.com/sites/its under IT Protocols and Guidelines.