BRANDON UNIVERSITY	**Information Technology Acceptable Use Policy (AUP)**	**Approved by:** President's Administrative Council **Administered by**: Chief Information Officer
Administrative Policy	**First Approved:** **January 11, 2006**	**Updated:** **June 16, 2022**

Brandon University ("the University") is committed to providing secure and high-quality Information Technology (IT) resources and services for all faculty, students, staff, and authorized external users and guests.

The University respects the privacy of all users of its IT resources and makes reasonable efforts to maintain confidentiality of Personal Information. The University monitors IT resources for malicious activity and may monitor the activity and accounts of individual users without notice, under any one or more of the following circumstances:

a. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the University or its IT resources, or to protect the University from liability.
b. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
c. There are reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

Access to Personal Information may be granted to an Authorized User, System Administrator, or agent to meet legitimate University business needs and operational requirements, or if an Authorized User is unavailable, or has their access revoked. Such access will be subject to the authorization of the Chief Information Officer or equivalent in consultation with the Associate Vice President People and Talent, Dean of Students, Provost, Vice President Administration and Finance, or President.

The University respects principles of academic freedom and open access to information for academic and teaching purposes. The free exchange of ideas is central to the educational process and the Information Technology Acceptable Use Policy supports this principle. The exceptions are uses that violate the law, endanger IT resources, or violate the policies articulated in this document.

1.0 Scope

The Information Technology Acceptable Use Policy (AUP) has been established to ensure the security and integrity of the University's IT resources, and fair and equitable access to those resources by all the members of the University community. The University is the sole owner and operator of the University's IT resources. Information Technology Services

("ITS") has a responsibility to maintain IT resources in a manner consistent with the University's mission.

This policy shall apply to all members of the University community, including faculty, staff, students, contractors, and authorized external users, and guests.

This policy governs the use of IT resources owned and operated by the University, including those purchased through research funds administered by the University or acquired by the University through a contractual agreement. "IT resources" is inclusive of all University computing systems, devices, and technologies including servers, desktops, laptops, laboratory computers, smart phones, networks and network devices, hardware, software, data, and applications related to these systems. This policy covers all University-owned IT resources, facilities, equipment, and services regardless of location or access site (on campus or off campus).

IT resources are intended to support research, education, instruction, and administrative processes of the University. Members of the University community using IT resources shall be aware they may have access to sensitive data in the course of their work and study and that such data should be appropriately managed and protected. Members of the University community should likewise be aware that improper usage of the University networks and systems could have adverse effects on other IT resources, facilities, and users at the University.

The policy has been developed in the context of, and is designed to complement:

- Existing University policies and regulations, particularly those governing use of University property and services, privacy, security, disciplinary aspects, respectful workplace compliance, non-academic misconduct, discrimination and harassment prevention, student records, copyright and intellectual property.
- Any Municipal, Provincial, and Federal Laws or Regulations.
- Collective agreements.

2.0 Policy

2.1 Authorized Use

a. University students, staff, faculty, visiting professors, researchers, or special presenters are entitled to the secure wireless network provided by the University.
b. Visitors and guests to the University are allowed access to the University's open, non-secure wireless network.
c. Users have access to the IT resources for which they are authorized.
d. Users are responsible for the use of their accounts and devices and shall keep their passwords and devices secure.

e. While this policy allows for reasonable personal use of University IT resources, the University is committed to the resources allocated for University related teaching, learning, research, and administrative work. The use of the IT resources for non-University-related activities that place heavy loads on University resources, causes network congestion, or that severely impacts the work of others is prohibited.
f. Users are responsible to follow the license agreements of the software they use and install. ITS may require users to obtain clarification from vendors on the responsibilities and limitations under software license agreements.

2.2 Breaches of Acceptable Use

Unless explicitly authorized (for instance, for purposes of study and research or for University business purposes) breaches of acceptable use include, but are not limited to:

a. Deliberate attempts to tamper with IT resources.
b. Attempting to circumvent information security provisions or exploit vulnerabilities, activities intended to disrupt normal University operations, IT resources, data security, networks, network security, hardware, or computer facilities.
c. Attempting unauthorized access to any IT resources.
d. Giving access to licensed or access-controlled IT resources to non-authorized persons.
e. Divulging passwords or credentials to any person, system, or third-party. ITS does not require access to users' passwords, nor does any other party.
f. Moving, modifying, or copying programs, or any other forms of software from one system to another without proper authorization. This includes personal computers, devices, and personal workstation software.
g. Use of software belonging to or licensed to other users or to Brandon University without proper authorization to do so.
h. Breaking or attempting to circumvent copyright, intellectual property, access, and licensing provisions.
i. Attempts to misrepresent or use other mechanisms to access restricted data.
j. Attempts to collect, use, or disclose, the personal information of others without informed consent of the other party.
k. Installation of network-enabled devices on the University's secure networks without authorization from ITS.
l. Use of University IT resources to create, display, distribute or disseminate threatening, discriminatory, harassing, abusive, or malicious material.
m. Use of University IT resources to send threatening, discriminatory, harassing, abusive, or malicious emails or messages.
n. Sending messages under an assumed name or modified address with intent to misidentify the sender or origin of the message.
o. The use of IT resources for personal business or commercial use, including but not limited to the posting of commercial web pages and the distribution of unsolicited advertising.
p. Use of IT resources for private consulting or for any form of direct personal financial gain.

q. Passwords used at the University shall not be used for any other system or service outside of Brandon University.

2.7 Consequences of Prohibited Use

a. The nature and severity of violations of this policy determines the level of initial response. Repeated violations of this policy following clear communication or warnings adds to severity of the response.
b. If the integrity or security of an IT resource is compromised or at-risk through suspected violation of this policy, ITS may direct the immediate removal of a user's access to IT resources pending completion of an internal investigation.
c. Examples of corrective actions and/or remedial actions may include one or more of the following:
    - Verbal or written warning from the appropriate supervisor/administrator
    - Formal apology
    - Mandated education or training
    - Community service
    - Loss of privileges
    - Probation
    - Restitution/alternative resolution
    - Interim suspension (with/without pay, pending an investigation) (removal from a course or part of a course)
    - Termination or expulsion or formal removal from campus
    - Specific for employees: change in work assignment
d. If violation of this policy is concurrent with violation of other University policies, then University Administrators may investigate the violation of all applicable policies and assign corrective action based on combined severity of all applicable policy violations.
e. If violation of this policy is concurrent with illegal actions, law enforcement will be notified.

3.0 Definitions

3.1 Access: The ability to view, use, edit information and data in IT resources.
3.2 Account: A system-generated user identification.
3.3 Authorized External User: An individual granted authorization to use IT resources owned by and operated by Brandon University but who is not an employee or student of the institution (e.g. invited speaker).
3.4 Facility: Any combination of IT resources or services, including physical spaces such as labs, or virtual services such as learning management systems.
3.5 Guest: A member of the public who is not an employee, student, or authorized external user of the institution (e.g. community user in the library, using wireless at Healthy Living Centre).
3.6 Hardware: The physical equipment used for networking and computing.

3.7 Information Technology (IT) Resources: Any information, data, software, hardware, research equipment, system, network, network enabled devices, facility, peripherals owned, leased, controlled, or operated by the University.

3.8 Messages: Electronically transmitted communication, including but not limited to emails, text messages, and chats.

3.9 Network: Any number of computers and devices joined together by a physical communications link which provides the roads for information traffic (e.g., sending files and e-mail) within an organizational environment, and allow users to access databases and share applications residing on servers.

3.10 Personal Information: Personal information as defined by Manitoba Freedom of Information and Protection of Privacy Act (FIPPA).

3.11 Software: The programs and other operating information used by a computer.

3.12 Users: Any individual that is using IT resources owned by and operated by Brandon University.

4.0 Review

Formal review of this policy will be conducted every three (3) years with the next scheduled review date June 2025. In the interim, this policy may be revised or rescinded if the President deems necessary or if there are changes within legislation which require such.

5.0 Referenced Policies

Brandon University Collective Agreements
Brandon University Discrimination and Harassment Prevention Policy and Procedures
Brandon University Sexualized Violence Policy
Brandon University Student Non-Academic Misconduct Policy
Guide to Internal Investigations at Brandon University
Brandon University's Student Records Policy
FIPPA (Freedom of Information and Protection of Privacy Act)

6.0 Related Procedures

ITS Procedures related to Account Provisioning
ITS Procedures related to Incident Management