Athabasca University

PROCEDURE

Acceptable Use of Information Technology Assets Procedure

Parent Policy	Security of Digital Information and Assets Policy		
Policy Sponsor	Vice President Information Technology and Chief Information Officer (VPIT & CIO)	**Category**	Administrative
Policy Contact	Chief Information Security Officer (CISO)	**Effective Date**	December 12, 2019
Procedure Contact	Chief Information Security Officer (CISO)	**Review Date**	December 12, 2024

1. Purpose

The purpose of this procedure is to outline the University's standards and requirements for the use of University IT Assets. The University is committed to maintaining an information technology environment that is supportive of the University's commitment to freedom of expression and is accessible, while also assuring the information technology resources are used responsibly, respectfully and in a manner that reflects high ethical standards, mutual respect and civility.

2. Scope

The University strives to foster and maintain an intellectual environment in which members of the University Community can access and create information, and collaborate with one another.

3. Definitions

Account	A means for accessing IT Assets that generally consists of an account name (or User ID) and associated Authentication method.
Asset Owner	University employee or member of Managed Security Services partner personnel to whom the Vice-President IT and CIO or CISO has delegated the authority to grant access to an IT Asset.
Authorized User	A person who has been granted access to an account and whom access has not been rescinded or terminated.
Digital Information or Content	Binary encoded information.

End-User Device	A computing device used by End-Users including desktop computers, net stations, laptops, and mobile devices (e.g., tablets, smart phones), monitors headphones and webcams.
Foreign Device	Any End-User Device that has not been issued or provided by Athabasca University, or that has not been approved for use by the VPIT&CIO.
Harassment	Any single incident or repeated incidents of objectionable or unwelcome conduct, comment, bullying or action by a person that the person knows, or ought reasonably to know, will or would cause offence or humiliation to another person or adversely affects another person's physical or psychological well-being. Harassment does not include the reasonable conduct or actions of the University in respect of the management of its Members. Harassment made on the basis of, or in relation to, a person's sexuality is Sexual Harassment.
Hazard	A situation, condition or thing that may be dangerous to health and safety.
IT Asset or Assets	Digital information and technology assets, which include: • Software (applications, database management, operating systems, licenses, etc.); • End-User Devices (portable storage devices, computers, laptops, tablets, smart phones, displays, net stations, etc.); • Digital Information; • Cloud-based or on-premise Servers (multi-user physical or logical computers, etc.); • Networks (cables, circuits, switches, routers, firewalls, etc.); and • Digital Storage Devices and Systems (cloud-based, removable or fixed devices that retain Digital Information, etc.) owned by, under the custody of, or commercially made available to, the University.
Privileged Account	An account that is authorized to a user who is trusted to perform security-relevant functions that ordinary users are not authorized to perform. The Authorized User of a Privileged Account also has the ability to control the access or permissions of other Authorized Users.
Security Incident (IT)	A digital security incident is indicated by a single or a series of unwanted or unexpected information security events that present a significant risk to the University's digital business operations and its IT Assets. Examples include, but are not limited to:

	• Disclosure or potential disclosure of identifying Sensitive Data or Information • Breaches of Data and Information Security Classifications. • Use of a Foreign End-User Device by a member of the University Community • Computer viruses or malware • Loss of laptops, tablets or smart phones containing Confidential Digital Information or Protected Information • Unauthorized access to IT Assets • Denial of online service attack • Cyber Security Incident • Criminal or Hostile State Act or activities Technology involving IT Assets.
Sexual Harassment	Any single incident or repeated incidents of objectionable or unwelcome conduct, comment, bullying or action by a person that the person knows, or ought reasonably to know, will or would cause offence or humiliation to another person or adversely affects another person's physical or psychological well-being made on the basis of, or in relation to, a person's sexuality. Sexual Harassment is considered a form of Sexual Violence.
Sexual Violence	A single incident or repeated incidents of violence, whether physical or psychological, that is threated, attempted or committed against a person without the person's consent through sexual means, coercion, or by targeting the person's sexuality. Sexual Violence includes, but is not limited to: • Sexual Assault; • Sexual Harassment; • Indecent exposure; • Voyeurism; • Degrading sexual imagery; and • Distribution of sexual images or video of a Member without their Consent.
Standard	A mandatory requirement, code of practice or specification.
Standard Operating Procedure (SOP)	A standard operating procedure addresses process-related information that is below the level of policies and procedures. Their content often inform the Policy Framework. A SOP is highly detailed, regularly revised and is deemed internal to the University, although a SOP may be shared on a need-to-know basis.

University Community	All faculty and staff, students, Board Members, contractors, postdoctoral fellows, volunteers, visitors and other individuals who work, study, conduct research or otherwise carry on business of the University.
User ID	A unique identifier assigned to an Authorized or Service to enable access to IT Assets.
Violence	The threatened, attempted or actual conduct of a person that causes or is likely to cause physical or psychological injury or harm.

4. Guiding Principles

4.1. Standards for Acceptable Use of IT Assets

a. Any member of the University Community, who witnesses misuse of University IT Assets should report it to the Chief Information Security Officer as soon as possible.

b. IT Assets must be used and managed in a responsible manner. Use of these resources in any manner that is disruptive, fraudulent, hazardous, harassing and threatening (e.g., sexual harassment or violence), obscene, racist, profane, pornographic or for malicious purposes is strictly prohibited.

c. Use of IT Assets for non-University commercial purposes or personal financial gain purposes is prohibited, including for, but not limited to: fundraising, bitcoin mining, soliciting participation in a social event not sponsored or endorsed by the University.

d. Any individual using IT Assets to create, access, transmit or receive University-related administrative information must protect that information and may not share it with any persons that are not employees of the university without written permission of the Vice President, University Relations or their appointed delegate.

e. End-User Devices must not be used to cross-connect a University network with a non-University network, that is, they may not be used to bridge two networks.

f. Foreign Devices must not be physically connected to a University network.

4.2. Access to IT Assets

a. Access to IT Assets will be provided only upon the documented consent of the VPIT & CIO or delegated IT Asset Owner.

b. Access to an IT Asset must be provided only where such access is necessary for the effective performance of personnel's duties.

4.3. Requirements for Authorized Use

a. Use of IT Assets is permitted only to Authorized Users. The use of User IDs and Authentication, is authorized only on an individual basis and may not be shared by multiple individuals.

b. Authorized Users are responsible for reasonable care of any University-owned End-User Devices provided to them.

c. Authorized Users must not share or disclose their Authentication credentials.

    i. Authorized Users must make all reasonable efforts to keep their User IDs and Authentication private and secure and follow IT practices (e.g., for password changes, resets, encryption, two-factor authorization).

d. Authorized Users may not enable or allow access to an IT Asset to anyone who is not an Authorized User of that IT Asset.

e. Authorized Users must stay within their authorized limits and refrain from seeking to gain unauthorized access to IT Assets beyond their permissions and privileges.

f. Authorized Users must respect intellectual property, copyrights, and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected Digital Information.

g. Authorized Users must respect the rights of other Authorized Users. They must not encroach on others' rights to use, access, and privacy.

4.4. General Use of IT Assets

a. University IT Assets are to be used for activities related to the mission of the University: teaching, learning, research and administration.

b. Limited personal use (i.e. use not related to the mission of the University) is permitted provided it complies with this procedure, does not compromise the business of the University, does not increase the University's costs, does not expose the University to additional risk, does not damage the University's reputation, and does not unduly impact the University's business and academic uses.

c. All other uses are prohibited.

4.5. Freedom of Expression

a. All forms of electronic communication are expected to reflect high ethical standards, mutual respect and civility and the University's commitment to freedom of expression. Authorized Users must refrain from transmitting inappropriate images, sounds or messages which might reasonably be considered harassing, fraudulent, threatening, obscene (e.g. pornographic) or defamatory; or material that is a violation of applicable law or University policy.

b. Authorized Users must be sensitive to the open nature of work areas and public University premises and take care not to display in such locations images, sounds or messages that are harassing, threatening, obscene (e.g. pornographic), defamatory, or that are a violation of applicable law or University policy.

4.6. Monitoring and Controlling for Acceptable Use

a. Inactivity timeout features on End-User Devices must be enabled so as to require Authentication to regain access to the End-User Device following expiry of the timeout period.

b. Authorized Users may not bypass or disable security or management functions mandated or installed by IT or its Managed Security Services partner on IT Assets.

c. Authorized Users may not modify an IT Asset except in accordance with established business processes and as required by their job duties and responsibilities.

   i. Any modified IT Asset must be logged for cybersecurity traceability and audit review processes

d. Asset Owners must review and confirm as appropriate access to, or possession of, IT Assets by each Authorized User at least once every twelve months.

e. Access to IT Assets must be disabled immediately upon the cessation of employment, contractual or other relationship with the University of an Authorized User.

   ii. Physical IT Assets must be returned to the appropriate manager upon cessation of a person’s employment, contractual or other relationship with the University.

iii. Access rights must be reviewed immediately upon any change in the status, role or relationship of an Authorized User relative to the University.

iv. Account passwords and Privileged Account passwords must be changed periodically in accordance with the frequency established by the CISO and documented in the Information and Communication Technology Account Management Procedure.

v. Passwords must comply with standards defined in the Information and Communication Technology Account Management Procedure.

4.7. Responding to and Reporting Inappropriate Use of IT Assets

a. Members of the University Community report all IT Security Incidents, including cyber security incidents without undue delay to the appropriate authority as defined in the IT Security Incident Response Procedure.

b. The University reserves the right to withhold and suspend access to its IT Assets to any individual if there are reasonable grounds to suspect that such access poses a threat to the operation or security of an IT Asset or the reputation of the University.

4.8. Requirements for Compliance

a. The University's actions under this procedure will be taken in accordance with the Code of Conduct.

b. Use of the University's IT Assets must comply with all applicable laws, University policies, procedures, appendices and guidelines

c. Non-compliance constitutes misconduct and may be handled under the applicable collective agreements, University policy, or law.

4.9. Collection and Use of IT Asset Use Information

a. The University will protect information against unauthorized disclosure.

b. The University reserves the right to access, monitor and record both stored or in-transit data and the usage of information technology resources when there is suspected or alleged impropriety, a business need for access in the absence of an employee, a request under the Freedom of Information and Protection of Privacy Act, or as otherwise required by law.

i. The University has the right to use information gained in this way in disciplinary actions as prescribed in University policies, and to provide such information to appropriate internal and external investigative authorities.

c. Access of this information when there is a suspected impropriety must be requested by the Chief Human Resources Officer or their appointed delegate to the Vice President IT and CIO or their appointed delegate.

d. Permission to access this information must come from the Vice President IT and CIO or their appointed delegate to the IT employee(s) that will provide assistance.

5. Applicable Legislation and Regulations

Copyright Act (Canada)
Criminal Code (Canada)
Canadian Human Rights Act
Charter of Rights and Freedoms
Freedom of Information and Protection of Privacy Act (FOIP Act)
Alberta Human Rights Act
Post-Secondary Learning Act
Occupational Health and Safety Act
Occupational Health and Safety Regulation

6. Related Procedures/Documents

Code of Conduct for Members of the University Community
Protection of Privacy Policy
Harassment, Violence, and Sexual Violence Policy
Information Technology Security Incident Response Procedure
Significant Cyber Security Incident Reporting Procedure
IT Service Catalog

NOTE: The subject matter and scope of this procedure are also supported by internal-use only Standard Operating Procedures.

History

Date	*Action*
December 12, 2019	Executive Team (Policy Approved)