Acceptable Use of Information and Communications Technology Assets Policy

Policy Sponsor:	Office of Vice-President Information Technology
Policy Contact:	Vice-President IT and CIO
Policy Number:	ITS-2
Effective Date:	June 10, 2016
Approval Group:	The Governors of Athabasca University
Approval Date/Motion #:	June 10 2016, Motion # 211-06
Review Date:	Annually

Purpose

The purpose of this policy is to define the University's expectations and requirements for the use of University ICT Assets.

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 colleagues and peers. As part of this effort, the University is committed to maintaining an information technology environment that is free from harassment and is accessible to its members.

Such an environment can only exist when all members use and manage the **information technology resources** responsibly, respectfully and in a manner that reflects high ethical standards, mutual respect and civility.

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

Definitions

Account	A means for accessing ICT Assets that generally consists of an account name (or User ID) and associated Authentication method.
Account Administrator	A designated employee trained in the use of University software systems for the purpose of performing domain account creation, deletion and deactivation.
Application	A software program that collects, manipulates, processes, stores, distributes, displays or prints Digital Information.
Archive	The relocation of Digital Information to a medium for long-term storage when such information does not need to be readily accessible, but may be needed in the future.
Asset Owner	An employee of the University to whom the Vice-President IT and CIO has delegated the authority to grant access to an ICT Asset. Asset Owners may delegate their authority to one or more employees of the University.
Authentication	A means of verifying the identity of an Authorized User.
Authorized User	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this policy.
Backup	The copying of Digital Information from one electronic medium to another.
Backup Copy	The copy of Digital Information made during Backup.
Confidential Digital Information	Information identified as confidential by the person to whom the responsibility for such designation has been delegated by the University.
Digital Information	Binary encoded information.
Digital Storage Device	A device that can retain binary encoded information in a permanent state.
Email Account	An Account used to send or receive email.

FOIP	Alberta *Freedom of Information and Protection of Privacy Act*.
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 University's Director of IT Operations.
General Service Account	A shared Account that is used for communication or information exchange between applications under Software control.
General Service Account Owner	A person who has been designated as having responsibility for the use of a General Service Account by the Vice-President IT and CIO or the Director of IT Operations.
ICT	Information and communication technology.
ICT Assets or **Assets**	Information Communication and Technology Assets, which include: • **Software** (applications, database management, operating systems); • **End User Devices** (portable storage devices, computers, laptops, tablets, smart phones, displays, net stations); • Digital Information; • **Servers** (multi-user physical or logical computers); • **Networks** (cables, circuits, switches, routers, firewalls); and • **Digital Storage Devices and Systems** (removable or fixed devices that retain Digital Information) owned by, under the custody of, or commercially made available to, the University.
ICT Incident or **Incident**	Any failure or malfunction of ICT Assets that results in a loss of Service to the University community.**:**
ICT Security Incident	Any event that has compromised, is suspected of having compromised, or is likely to compromise the confidentiality, integrity or availability of Athabasca University's ICT Assets. Examples include, but are not limited to: • Computer viruses or malware; • Loss of laptops, tablets or smart phones containing Confidential Digital Information or Protected Information; • Unauthorized access to ICT Assets; • Denial of online service attack; and

	• Criminal activities involving ICT Assets. An equipment or software performance issue, failure or malfunction is NOT considered an ICT Security Incident if there is no indication that it was caused intentionally.
Incident Manager	An individual designated to assign personnel to, coordinate the response to, and issue a report regarding an ICT Security Incident or ICT Incident.
ITS	Information Technology Services department of the University.
Life Cycle	The span of time between the creation of an ICT Asset and its disposal.
Open Access Asset	An ICT Asset that can be accessed without the need for prior approval from the Asset Owner.
Privileged Account	An Account that provides an Authorized User with the ability to control the access or permissions of other Authorized Users.
Protected Information	Information that is protected under some legislation.
Recovery	The restoration of point-in-time copies of Digital Information from a Backup Copy.
Responder	A staff member assigned by an Incident Manager to investigate an ICT Security Incident or ICT Incident.
Service	An integrated group of ICT Assets that provides value to Authorized Users.
Security Incident Report	A written report using the approved ICT Security Incident Report Form.
System Administrator	A University employee who is responsible for the upkeep, configuration and reliable operation of ICT Assets.
User ID	A unique identifier assigned to an Authorized User or Service to enable access to ICT Assets.
VPIT and CIO	Vice-President Information Technology and Chief Information Officer of the University.

Policy Statements

1. University ICT Assets are to be used primarily for activities related to the mission of the University, including, but not limited to teaching, learning, research and administration. Limited personal use (i.e. use not related to the mission of the University) is permitted provided it complies with this Policy, 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. All other uses are prohibited.

2. ICT Assets must be used and managed in a responsible manner. Use of these resources for disruptive, fraudulent, harassing, threatening, obscene, racist, profane, pornographic or malicious purposes is strictly prohibited. Use of ICT Assets for non-University commercial purposes is prohibited.

3. Application and enforcement of this policy shall not in any way, constrain academic freedom.

4. Use of ICT Assets other than Open Access Assets is permitted only to Authorized Users. Unless otherwise stated, such access, including the use of User IDs and Authentication, is authorized only on an individual basis and may not be shared by multiple individuals. Authorized Users must make all reasonable efforts to keep their User IDs and Authentication private and secure.

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

6. Any individual using ICT Assets to create, access, transmit or receive University-related information must protect that information in a manner that is commensurate with its value, use, and sensitivity.

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

8. All forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility. 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.

9. 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.

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

11. The University will protect information against unauthorized disclosure. 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. 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.

12. Anyone witnessing use of University ICT Assets in a manner that contravenes this policy should report it to a Vice President, Dean or Director.

13. Athabasca University's students, employees and contractors must report all ICT Security Incidents without undue delay to the appropriate authority as defined in the ICT Security Incident Response Procedure.

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

15. The University's actions under this policy will be taken in accordance with the *Code of Conduct*

16. System Administrators have the responsibility to investigate and take action in the case of suspected or alleged unacceptable use. With the approval of their supervisor and with due regard for the rights of users' privacy and the confidentiality of users' data, System Administrators have the right to suspend or modify Authorized Users' access to ICT Assets. System Administrators have the responsibility to take immediate action in the event the University is at imminent risk. System Administrators may examine files, passwords, accounting information, data, and any other material that may aid in an investigation of possible abuse.

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

Applicable Legislation and Regulations

Copyright Act (Canada), R.S. 1985, c. c-42
Criminal Code (Canada), R.S. 1985, c. c-46
Code of Conduct

Related References, Policies, Procedures and Forms

Athabasca University Code of Conduct
Protection of Privacy Policy
ITS Services Catalogue (under development)

History

The Board of Governors, Athabasca University, June 10, 2016, Motion # 211-06 (approved)