Security and Protection of Digital Information and Information and Communications Technology Assets Policy

Policy Sponsor:	Office of Vice-President Information Technology (OVPIT)
Policy Contact:	Vice-President IT and CIO
Policy Number:	NA
Effective Date:	June 10, 2016
Approval Group:	The Governors of Athabasca University
Approval Date:	June 10, 2016, Motion # 211-08
Review Date:	Annually
Procedures:	Digital Information Backup Procedure Disposal of Information and Communication Technology Assets Procedure Information and Communication Technology Account Management Procedure Information and Communication Technology Incident Response Procedure

Purpose

The purpose of this policy is to ensure the privacy and security of digital information and to protect the ICT Assets of Athabasca University (the University). The policy applies to all employees, associates, and contractors of the University to whom access to ICT Assets has been granted. This policy does not apply to student use of ICT Assets while they are in pursuit of their studies with the University. This policy does not apply to Open Access Assets.

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Authorized User	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this policy.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. Authorized Users are responsible for reasonable care of any End User Devices provided to them.
2. End User Devices may 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.
3. Foreign Devices may not be physically connected to a University network.

4. Access to ICT Assets

    4.1. ICT Assets may only be accessed using an Authentication method appropriate to the value, sensitivity, and confidentiality of the Asset.

    4.2. Access to ICT Assets (other than Open Access Assets) will be provided only upon the documented consent of the ICT Asset Owner.

    4.3. Authorized Users may not enable or allow access to an ICT Asset that is not an Open Access Asset to anyone who is not an Authorized User of that ICT Asset.

    4.4. Access to an ICT Asset must be provided only where such access is necessary for the effective performance of a person's University duties.

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

    4.6. Authorized Users may not bypass or disable security or management functions mandated or installed by ITS on ICT Assets.

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

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

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

    4.10. Physical ICT Assets must be returned to the appropriate manager upon cessation of a person's employment, contractual or other relationship with the university.

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

    4.12. Account passwords and Privileged Account passwords must be changed periodically in accordance with the frequency established by the Director of IT Operations and documented in the Information and Communication Technology Account Management Procedure.

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

5. Retention and disposition of Digital Information must comply with the standards defined in the University's Records Management Policy.

6. Confidential Digital Information and Protected Information

    6.1. Confidential Digital Information and Protected Information may only be stored on ICT Assets.

    6.2. Confidential Digital Information and Protected Information may only be stored on an End User Device in an encrypted form.

    6.3. Confidential Digital Information and Protected Information may only be transmitted in an encrypted form or over a secure network link.

7. Disposal of ICT Assets

    7.1. ICT Assets with the exception of Digital Information will be disposed of in accordance with procedures established by the Vice-President IT and CIO.

    7.2. The disposal process for Digital Storage Devices will ensure all Digital Information is removed prior to disposal.

8. 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.

9. Subject to provisions in other policies, legal agreements or legislation, Digital Information is the property of the University.

10. Some employees and contractors, by virtue of their responsibilities and in the normal execution of their duties, have access to Confidential Digital Information or Protected Information, or Digital Information that would normally be considered confidential. These individuals may not disclose such information during or after their employment with, or their provision of services to, the University has ended.

11. Unauthorized access to ICT Assets is prohibited. Any unauthorized attempt to circumvent controls put in place to protect ICT Assets is prohibited.

12. The VPIT and CIO will ensure that an independent audit of ICT Asset security is completed each year. The results of this audit will be provided to the Audit Committee of the Board of Governors.

13. Only the Vice-President IT and CIO or President can authorize exceptions to this policy, and only in cases where such action serves the interests of the University.

14. Suspected violations of this policy may result in immediate suspension or restriction of privileges.

15. Violations of this policy may result in discipline or, in the event of serious violation, dismissal. Any disciplinary action including dismissal shall be taken in accordance with, and be subject to, the provisions of the relevant collective agreement, where applicable.

Applicable Legislation and Regulations

Alberta *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25
Copyright Act (Canada), R.S. 1985, c. c-42
Criminal Code (Canada), R.S. 1985, c. c-46
Code of Conduct enacted pursuant to the *Public Service Act*

Related References, Policies, Procedures and Forms

Athabasca University Code of Conduct
Conflict of Interest Policy
Digital Information Backup Procedure
Disposal of Information and Communication Technology Assets Procedure
Information and Communication Technology Account Management Procedure
Information and Communication Technology Incident Response Procedure
Protection of Privacy Policy
Records Management Policy

History

The Board of Governors Athabasca University, June 10, 2016, Motion # 211-08(approved)