Information and Communication Technology Security Incident Response 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/Motion #:	June 10, 2016, Motion # 211-07
Review Date:	Annually
Procedures:	Information and Communication Technology Security Incident Response Procedures

Purpose

This policy is intended to ensure that all Information and Communication Technology (ICT) Security Incidents affecting information and communications technology assets (ICT Assets) of Athabasca University (the University) are handled in a timely, structured, and consistent manner that complies with relevant regulations and legislation and that protects the University's reputation.

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Authorized User:	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this policy.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:	Information stored in ICT Assets using binary encoding.
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. 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 Procedure.
2. The Vice-President IT and CIO will be responsible for managing and coordinating responses to ICT Security Incidents
3. The Vice-President IT and CIO may delegate responsibility for ICT Security Incident responses as appropriate.
4. The University FOIP Coordinator must be notified of an ICT Security Incident where Confidential Digital Information or Protected Information has been or is believed to have been disclosed to unauthorized persons or organizations.
5. If there is reason to believe any person vested with authority or responsibility under this policy or its related procedure is the cause of an ICT Security Incident, the authority and responsibilities of that individual will fall to that individual's immediate supervisor.

6. The Vice-President IT and CIO has the right to seize or disrupt communications from ICT Assets that are involved in an ICT Security Incident.
7. The Vice-President IT and CIO will report ICT Security Incidents of significant impact to the University President and University Secretary and appropriate executive committee members as determined by the nature of the ICT Security Incident.
8. The University Secretary is responsible for initiating contact with legal counsel and law enforcement agencies as appropriate.
9. The Vice-President IT and CIO and the University Secretary must approve any forensic investigation related to an ICT Security Incident.
10. All individuals involved in an ICT Security Incident response, or digital evidence collection, or both, must maintain the confidentiality of the activities performed and information collected on a need-to-know basis.
11. The Vice-President IT and CIO, or designate, must approve any actions in response to an ICT Security Incident that have the potential to disrupt University ITS operations.
12. 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 *Electronic Transaction Act*.
Alberta *Freedom of Information and Protection of Privacy Act*.
Copyright Act (Canada)
Criminal Code (Canada)

Related References, Policies, Procedures and Forms

Information and Communication Technology Security Incident Response Report Form.
Information and Communication Technology Security Incident Response Procedure
Conflict of Interest Policy
Protection of Privacy Policy

History

The Governors of Athabasca University, June 10, 2016, Motion # 211-07 (approved)