Information and Communication Technology Incident Response Procedure

Policy Sponsor:	Office of Vice-President Information Technology (OVPIT)
Name of Parent Policy:	Security and Protection of Digital Information and Information and Communications Technology Assets Policy
Policy Contact:	Vice-President IT and CIO
Procedure Contact:	Director of IT Operations
Effective Date of Procedures:	June 10, 2016
Review Date:	Annually

Purpose

The purpose of this procedure is to provide direction to Athabasca University (University) staff when dealing with failures or malfunctions affecting any ICT Asset.

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Authorized User	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this procedure or this procedure's parent policy.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 person 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.

Procedure

When an ICT Asset failure or malfunction is suspected to have occurred or is occurring, members of the user community should notify the ITS help desk. The ITS help desk will immediately notify the Director of IT Operations or designate.

The Director of IT Operations or designate will name an Incident Manager, who will be responsible for assigning Responder(s) to the Incident and coordinating their activities.

The ITS help desk will post the Service outage information to the system status page of both the intranet and internet sites of the University or initiate a fan-out call to inform internal users of the outage. Public facing Services will have a failover mechanism in place to display a static status page that will indicate that the Service is temporarily unavailable. Notification and escalation to other parties will be based on the notification and escalation schedules in the ITS Services Catalogue. Where applicable, the Office of Advancement will be informed of the outage so that they may monitor and respond to student reactions via social media.

Responders' first objective is to restore the Service by:

- determining the extent of the outage and the ICT Assets that have failed or malfunctioned;
- repairing or replacing the failed or malfunctioning ICT Assets;
- switching to backup systems where available;
- establishing a workaround that my include manual processes; and
- authorizing, where applicable, the purchase of replacement parts.

Responders must document all actions taken in responding to the ICT Incident including the date and time that each action was taken.

The Incident Manager will ensure that the root cause of the outage is investigated. The Incident Manager is responsible for collecting all relevant documentation prior to completing an ICT Incident Report. All ICT Incident Reports not containing sensitive, protected or confidential information will be posted to the ITS website.

In the event the ICT Incident resulted in the loss of data, the University Secretary and Vice-President IT and CIO must be informed immediately. The University Secretary will determine the need for notification to others within the University community.

Applicable Legislation and Regulations

Alberta *Freedom of Information and Protection of Privacy Act*

Related References, Policies, Procedures and Forms

Security and Protection of Digital Information and Information and Communications Technology Assets Policy
Information and Communication Technology Incident Report
ITS Services Catalogue
Protection of Privacy Policy

History

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