Information and Communication Technology Security Incident Response Procedure

Policy Sponsor:	Office of Vice-President Information Technology (OVPIT).
Name of Parent Policy:	Information and Communication Technology Security Incident Response 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 students and staff of Athabasca University (the University) when dealing with security incidents affecting any ICT 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A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this procedure or this procedure's parent policy.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

1.0 Notification

1.1 Athabasca University’s students, employees and contractors must report all ICT Security Incidents without undue delay.to the ITS Help Desk. The ITS help desk will notify the Director of IT Operations or Vice-President IT and CIO or their designate of ICT Security Incidents impacting more than one Authorized User and ICT Security Incidents involving disclosure or potential disclosure of Confidential Digital Information or Protected Information to unauthorized persons or organizations.

1.2 The Director of IT Operations or Vice-President IT and CIO or their designate to whom the ICT Security Incident has been reported will notify the FOIP Coordinator of ICT Security Incidents involving disclosure or potential disclosure of Confidential Digital Information or Protected Information to unauthorized persons or organizations.

2.0 Response

2.1 The individual to whom the ICT Security Incident has been appropriately reported will either assign an Incident Manger or assume the responsibilities of the Incident Manager. The Incident Manager will assign Responders as appropriate and coordinate their activities

2.2 Responders must investigate to determine the cause of the event and report to the Incident Manager if the event is confirmed to be an ICT Security Incident.

2.3 Should the event be confirmed as an ICT Security Incident appropriate containment activities, if required, should be initiated by the Incident Manager.

2.4 Containment involves ensuring that unauthorized access resulting from the ICT Security Incident is prevented while preserving evidence that may be required to determine the root cause. The measures required for effective containment will vary depending on the technology involved and the infrastructure available.

2.5 In the event that a Service must be disabled to effect containment of the ICT Security Incident, the following must take place prior to the Service being brought back into operation:

2.5.1 All affected Software must be deleted and re-installed.

2.5.2 All passwords granting access to the affected ICT Assets must be changed.

2.5.3 All passwords stored on the affected ICT Assets that are used to access other systems, such as remote database servers, must be changed.

2.5.4 Private keys stored on the affected ICT Asset must be discarded and corresponding public keys must be removed from other ICT Assets. Key pairs must be regenerated

2.6 In any case, where action(s) to contain an ICT Security Incident result in the interruption of a Service, the Incident Manager must ensure that all support personnel involved in supporting the Service are notified as soon as possible and, where applicable, notifications are broadcast to the user community.

3.0 Reporting

3.1 Over the course of the investigation, Responders must, at a minimum, provide daily reports to the Incident Manager. Where the ICT Security Incident involves Confidential Digital Information or Protected Information or where the exposure of such information is imminent, the Incident Manager must involve the FOIP Coordinator as early as possible in the investigation.

3.2 All actions taken by the Responder(s) must be recorded and include the date and time that each action was taken.

3.3 Once the ICT Security Incident has been identified, corrected, mitigated, or contained, the Incident Manager must prepare an ICT Security Incident Report, containing all the details relating to the ICT Security Incident, actions taken, lessons learned and, where applicable, recommendations pertaining to improvements to security measures and system management practices in place at the time of the incident.

3.4 The Incident Manager will distribute the ICT Security Incident Report to the Vice-President IT and CIO and others as deemed appropriate.

3.5 Where Confidential Digital Information or Protected Information is a factor in the ICT Security Incident, the ICT Security Incident Report will also be distributed to the FOIP Coordinator.

Applicable Legislation and Regulations

Alberta *Freedom of Information and Protection of Privacy Act*
Criminal Code (Canada)

Related References, Policies, Procedures and Forms

Information and Communication Technology Security Incident Response Policy
Information and Communication Technology Security Incident Report Form
Protection of Privacy Policy

History

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