Athabasca University

PROCEDURE

Information Technology Security Incident Response Procedure

Parent Policy	Security of Digital Information and Assets Policy		
Policy Sponsor	Vice President Information Technology and Chief Information Officer (VPIT & CIO)	**Category**	Administrative
Policy Contact	Chief Information Security Officer (CISO)	**Effective Date**	December 12, 2019
Procedure Contact	Chief Information Security Officer (CISO)	**Review Date**	December 12, 2024

1. Purpose

The purpose of this procedure is to provide an overview of the actions University IT employees take when dealing with security incidents affecting any IT Assets.

2. Scope

This procedure applies to all IT Security Incidents in general. All members of the University Community are expected to report apparent IT threats. Cyber Security incidents are addressed through a separate, complimentary procedure. The specifics of any actions taken to address Security Incidents follow Standard Operating Procedures (SOPs) that are not public information and are on a need-to-know basis only as determined by the Chief Information Security Officer and the VPIT & CIO.

3. Definitions

Confidential Digital Information	Information identified as confidential or Protected B Classification as per the Data Classification procedure of the Information Management Policy.
End-User Device	A computing device used by End-Users including desktop computers, net stations, laptops, and mobile devices (e.g., tablets, smart phones), monitors headphones and webcams.
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.
IT Asset or Assets	Digital information and technology assets, which include: • Software (applications, database management, operating systems, licenses, etc.); • End-User Devices (portable storage devices, computers, laptops, tablets, smart phones, displays,

	net stations, etc.); • Digital Information; • Cloud-based or on-premise Servers (multi-user physical or logical computers, etc.); • Networks (cables, circuits, switches, routers, firewalls, etc.); and • Digital Storage Devices and Systems (cloud-based, removable or fixed devices that retain Digital Information, etc.) owned by, under the custody of, or commercially made available to, the University.
IT Incident	Any failure or malfunction of IT Assets that results in a loss of Service to the University Community.
Protected Information	Information that is protected as per the Data Classification procedure of the Information Management Policy.
Security Incident (IT)	Security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A digital security incident is typically indicated by a single or a series of unwanted or unexpected information security events that present a significant risk to Athabasca University's digital business operations and its IT Assets. Examples include, but are not limited to: • Disclosure or potential disclosure of identifying Sensitive Data or Information • Breaches of Data and Information Security Classifications. • Use of a Foreign End-User Device by a member of the University Community • Computer viruses or malware • Loss of laptops, tablets or smart phones containing Confidential Digital Information or Protected Information • Unauthorized access to IT Assets • Denial of online service attack • Cyber Security Incident • Criminal or Hostile State Act or activities Technology involving IT Assets.
Sensitive Data and Information	Sensitive data is associated with a person and is typically identifying. Any data or information that reveals: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; and data concerning health or a natural person's sex life and/or sexual orientation.
Standard Operating Procedure (SOP)	A standard operating procedure addresses process-related information that is below the level of policies and procedures. Their content often inform the Policy Framework. A SOP is highly detailed, regularly revised and is deemed internal to the

	University, although a SOP may be shared on a need-to-know basis.
University Community	All faculty and staff, students, Board Members, contractors, postdoctoral fellows, volunteers, visitors and other individuals who work, study, conduct research or otherwise carry on business of the University.
VPIT and CIO	Vice-President Information Technology and Chief Information Officer of the University.

4. Guiding Principles

4.1. The declaration of a Security Incident will be accompanied by a Security Condition level determined utilizing conditions as determined by a SOP threat escalation protocol and security incident prioritization table.

4.2. The Security Incident Response Lead has the authority, in consultation with the VPIT & CIO, and Security Incident Response Team to take any, and all, actions required in the detection, analysis, containment, eradication and recovery of the University's digital systems during a declared security incident.

4.3. The Security Incident Response Lead is the only individual who may declare a security incident and the corresponding closure of a security incident.

4.4. Any event that compromises, is suspected of having compromised, or is likely to compromise the security of the University's IT environment or assets necessitates immediate response.

4.5. The University Community must immediately report all security incidents; suspected, or otherwise; including but not limited to:

a. Unauthorized University computer access or use by third parties;

b. Loss of system functionality –especially after having accessed a website, or receiving and acting on an unsolicited email; and

c. Unauthorized University office access by any non-University third party.

4.6. The University Community will:

a. Cooperate with the Security Incident Response team during investigations of security incidents by providing all requested information whether verbal or written to members of the team in a timely manner.

b. Participate in post-incident triggered training to become aware of new lessons learned.

c. Implement, or take follow-up actions, as indicated in training reports from security incident responder's investigation.

d. Maintain proper security controls and adhere to the University security policies.

4.7. The Chief Information Security Officer (CISO) is responsible for managing and coordinating responses to Security Incidents.

4.8. IT will establish a Security Incidence Response Team whose primary roles will be to support overall IT security by aligning all Security Incident program activities with University Policies, Procedures and Standard Operating Procedures.

4.9. The Security Incidence Response Team will execute its mandate under the authority of the University's Digital Governance Security Subcommittee (DGSS). All individuals involved in Security Incidence Response, or digital evidence collection, or both, must maintain the confidentiality of the activities performed and information collected on a need-to-know basis.

5. Applicable Legislation and Regulations

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

6. Related Procedures/Documents

Protection of Privacy Policy
Significant Cyber Security Incident Reporting Procedure
Data and Information Security Classification Procedure
Information Technology Service Management Procedure
Alberta Association in Higher Education for Information Technology's ITM Control Framework

NOTE: The subject matter and scope of this procedure are also supported by internal-use only Standard Operating Procedures.

History

Date	*Action*
December 12, 2019	Executive Team (Policy Approved)