Athabasca University

PROCEDURE

Significant Cyber Security Incident Reporting 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

This procedure outlines the University's approach to address the threat environment that puts the complex technology systems associated with 100% digital University at risk. The risks associated with Cyber Security are constantly evolving and becoming sophisticated and targeted, and the University conforms to the expectations of the Cyber Security Incident Reporting Guideline issued by the Government of Alberta in 2018.

2. Scope

The scope of this procedure applies to any significant Cyber Security incident and for the purposes of collaboration across the post-secondary systems may apply to lesser incidents. The Chief Information Security Officer is responsible for incident management processes, and all members of the University Community are expected to report apparent Cyber Security threats.

3. Definitions

Cyber Security	The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. Cyber Security incidents have the potential to compromise the confidentiality, integrity, availability, reliability and value of information and related information technology (IT) assets. Incidents also have the potential to cause injury to students, employees or other individuals.
DevSecOps Practice	Building security into all aspects of the technology lifecycle and its assets into requirements, into design, into code, and into deployment, logging and monitoring. *DevSecOps=Development, Security and Operations*

Significant Cyber Security Incident	An incident which has one or more of the following characteristics: • Has a medium to high impact on the standard operation of services within the University; • May be a breach or violation of policy or standards and; • May occur inadvertently or deliberately.
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.

4. Guiding Principles

4.1. The IT Security Incident Procedure Guiding Principles may also be applied to Cyber Security Incidents. Additionally, the University will validate how it manages Cyber Security incidents with clear and comprehensive Standard Operating Procedures and DevSecOps practices communicated internally.

4.2. When warranted, the University will collaborate with others in the post-secondary system, industry and intelligence services to improve overall system responses to such threats.

4.3. Specific procedural content addressing components of Cyber Security incident reporting to the Government of Alberta including: assessment criteria related to impact severity of a cyber threat; notification requirements; reporting requirements; and, communication requirements are followed in accordance with the Government of Alberta Cybersecurity Incident Report Guidelines for Post-Secondary as finalized by Advanced Education in 2018.

4.4. If warranted, by incident severity, the Chief Information Security Officer and VPIT & CIO will produce the appropriate notifications and final reports to the Government of Alberta personnel as per the Government of Alberta Cybersecurity Reporting Guidelines for Advanced Education.

4.5. The VPIT & CIO must approve any forensic investigations related to Cyber Security Incidents.

5. Applicable Legislation and Regulations

Alberta Public Agencies Governance Act – sections 8 and 12(d)
Freedom of Information and Protection of Privacy Act
Criminal Code (Canada)

6. Related Procedures/Documents

Information Technology Security Incident Response Procedure

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)