Athabasca University

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
Approved By	Executive Team	**Review Date**	December 12, 2024
Approved Date	December 12, 2019		

1. Purpose

Athabasca University is a 100% digital University. Security is an inherent component of being a digital University and is therefore integral to all aspects of IT life cycle management. IT security risks and Cyber Security threats will be minimized through a set of strategies that prevents unauthorized access to the University's digital information and technology assets. IT security will also maintain the integrity and confidentiality of data and information, blocking access by sophisticated hackers. Taken together, these efforts enable the realization of the University's business objectives including operating and offering its services, even in the presence of adverse conditions.

2. Scope

All digital information and technology assets associated with the University's operations and business continuity services are included in the scope of this policy. The requirements to secure and protect digital information and technology assets together with the management of associated risks are essential components of Digital Governance. As such, IT security is complemented by other Digital Governance Framework's policies, procedures and DevSecOps Practices. The policy applies to all members of the University Community who have access to the University's Digital information and technology assets (e.g., IT infrastructure, software, End-User Devices, platforms, etc.), and from whom acceptable usage behaviour is expected.

3. Definitions

Account	A means for accessing digital information and technology assets that generally consists of an account name (or User ID) and associated Authentication method.

Authentication	A means of verifying the identity of an Authorized User, including by two-factor identity verification.
Authorized User	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this policy.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.
Board Audit Committee	Assists the Board in fulfilling its due diligence, fiduciary, financial reporting and audit responsibilities and to approve, monitor, evaluate and provide advice on matters affecting the external audit, internal audit, risk management, legal and regulatory compliance, and the financial reporting and accounting control policies and practices of the University.
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 digital information and technology (IT) assets. Incidents also have the potential to cause injury to students, employees or other individuals.
Data	The terms data, information, and knowledge are frequently used for overlapping concepts. The main difference is in the level of abstraction being considered. Data is often the lowest level of abstraction.
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*
Digital Information or Content	Binary encoded information.
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.
Lifecycle (IT)	The span of time between the creation of a technology or digital asset and their disposal.
Lifecycle Management	In IT this model refers to how something is planned, managed and monitored from inception to completion, including evergreening.
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 Actor activities Technology involving IT Assets.
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.

4. Guiding Principles

4.1. General

a. All guiding principles are intended to guide expected behaviours associated with the use of digital information and technology assets, Account Management, Digital Information Backup and Disposal, and preparing for IT security risks, addressing Security Incidents and Cyber Security threats or breaches.

b. The University strives to foster and maintain an intellectual environment in which members of the University Community can access and create information, and collaborate with students, colleagues and peers. As part of this effort, the University is committed to maintaining an information technology environment that is supportive of the University's commitment to freedom of expression and is accessible to its members.

c. This policy and its procedures meet the organization's needs based on known levels of risk and risk tolerance, and such as are integral to enterprise risk management.

d. Risk and threat assessments will ensure IT security strategies mature accordingly to defend and protect the University.

4.2. Authorized Access and Acceptable Use

a. Access to digital information and technology assets must be authorized and their acceptable use must reflect an understanding of their value, sensitivity, and confidentiality of the Asset.

b. Digital information and technology assets may only be accessed using an Authentication method appropriate to the value, sensitivity, and confidentiality of the Asset. Unauthorized access is prohibited.

c. All members of the University Community must use and manage digital information and technology assets responsibly, respectfully and in a manner that reflects high ethical standards, mutual respect and civility.

d. Generally speaking, the University's digital information and technology assets are to be used for activities related to the mission of the University: teaching, learning, research and administration. Any use must be mindful of risks that:

   i. Compromise the business of the University;
   ii. Increase the University's costs;
   iii. Expose the University to additional risk;
   iv. Damage the University's reputation, and;

v. Unduly impacts the University's business and academic interests.

4.3. Secure Storage, Classification, Backup and Disposal

a. Digital Information and Data secured under this policy are to be regarded and managed as valuable assets that must be protected through Lifecycle Management, and in accordance with its criticality, confidentiality, and future value potential.
b. Digital Information and Data stored in the Athabasca Cloud has multiple levels of security including, but not limited to, how access to the data is assigned and logged and how data is encrypted both at rest and in transit.
c. Security classifications associated with digital information not intended for public access are managed under the Data and Information Security Classification Procedure.
d. Backup plans for all digital information and technology assets are required in accordance with the Digital Information Backup Procedure to avoid data loss and restore operations if required.
e. All Digital Information will be disposed of in accordance with the IT Asset Disposal Procedure.

4.4. Security Incident Management

a. The University is committed to continuous vigilance and readiness through an incident management approach ensures overall IT security. Any IT Security Incidents, including Cyber Security incidents, affecting Athabasca University are handled in a timely, structured, and consistent manner that protects the University's reputation.
b. The Chief Information Security Officer is responsible for incident management processes, and all members of the University Community are expected to report apparent IT security threats.
c. Procedures related to this policy will mitigate threats and ensure the security of any digital assets. Digital information assets that are involved in Identity Management must be protected and secured at all times.

4.5. Authorities and Accountabilities

a. Overall compliance with legislation, regulations and contractual requirements is expected. Understanding and incorporation of these concepts into the design, implementation and evolution of programs, systems and services as well as daily practices as part of a DevSecOps Practice management approach.
b. Suspected violations of this policy may result in discipline or restriction of privileges. In the event of a serious violation, disciplinary action may

include immediate dismissal in accordance with applicable policies of the Corporate Human Resources Office, and/or applicable Collective Bargaining Agreements.

c. The CISO will ensure that an independent security audit of digital information and technology assets is completed each year. The results of this audit will be provided to the Board Audit Committee.
d. Only the Vice-President IT and CIO or President can authorize exceptions to this policy, and only in cases where such action serves the interests of the University.

5. Applicable Legislation and Regulations

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

6. Related Procedures/Documents

AUPE/The Governors of Athabasca University (the Board) Collective Agreement
CUPE/The Governors of Athabasca University (the Board) Collective Agreement
AUFA/The Governors of Athabasca University (The Board) Collective Agreement
AUGSA/The Governors of Athabasca University (The Board) Collective Agreement
Code of Conduct for Members of the University Community
Digital Enterprise Architecture Policy
Technology Management Policy
Information and Data Management Policy and Procedures
Protection of Privacy Policy
Records Management Policy
Acceptable Use of Information Technology Assets Procedure
Digital Information Backup Procedure
Disposal of Information Technology Assets Procedure
Account Management Procedure
Information Technology Security Incident Response Procedure
Significant Cyber Security Reporting Procedure
Identity Management Procedure
Information Technology Risk Management Procedure
Alberta Association in Higher Education for Information Technology's ITM Control Framework

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

History

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