Athabasca University

PROCEDURE

Digital Information Backup 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	Deputy CIO	**Review Date**	December 12, 2024

1. Purpose

This procedure defines a sound Backup framework for all IT systems at Athabasca University that will minimize security and business continuity risks associated with Digital Information loss.

2. Scope

These procedures apply to all University data stored in digital formats.

3. Definitions

Backup	The copying of Digital Information from one electronic medium to another.
Lifecycle Management	In IT this model refers to how something is planned, managed and monitored from inception to completion, including evergreening.
Recovery	The restoration of point-in-time copies of Digital Information from a Backup Copy.
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. To assure operational resilience, all data that meet sensitivity classification requirements must be stored in high resilience and availability zones.

4.2. Availability zones will be situated in geographically diverse regions powered by different power grids.

4.3. Technical backup policies related to automated backup schedules, retention management, and lifecycle management must be governed by business continuity, disaster recovery and operational and service level agreement requirements

4.4. Written procedures to support recovery point and recovery time objectives will be created and maintained according to business continuity practices.

a. Backup types and frequencies should reflect business requirements.

b. Backups will reflect the security requirements of data as well as its criticality to the University.

4.5. To align with data classification requirements, backups must be protected commensurate to sensitivity requirements as defined by data encryption and transmission procedures and standards.

4.6. Backup activity logs will be created and retained as dictated by records management policies, to support operational requirements, and to ensure audit trails are available.

4.7. Backup management must be PCI and ISO compliant.

4.8. Accurate and detailed records of all backup copies shall be retained and protected per data sensitivity definitions. Procedures to support restoration must also be created.

4.9. Backup management will be routinely tested as part of Disaster Recovery test scenarios.

5. Applicable Legislation and Regulations

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

6. Related Procedures/Documents

Security of Digital Information and Assets Policy
Protection of Privacy Policy
Records Management Policy

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)