Digital Information Backup Procedure

Policy Sponsor:	Office of Vice-President Information Technology (OVPIT)
Name of Parent Policy:	Security and Protection of Digital Information and Information and Communications Technology Assets
Policy Contact:	Vice-President IT and CIO
Procedure Contact:	Director of IT Operations
Effective Date of Procedures:	June 10, 2016
Review Date:	Annually

Purpose

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

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Authorized User	A person who has been granted access to an Account and for whom access has not been rescinded or terminated per this procedure or this procedure's parent policy.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 GENERAL

1.1. Backup will occur every business day, scheduled to minimize impact to Authorized Users. The frequency and nature of Backup may be modified by the Director of IT Operations when required.

1.2. The Backup and Recovery processes for each Digital Storage Device must be documented in the Backup schedule and reviewed at least annually by the Director of IT Operations.

1.3. Backup must include verification that confirms the integrity of the Backup Copy contents.

1.4. Assigned ITS personnel must monitor all Backup attempts and review the Backup process outcome to determine whether all Backups were successful each business day. A Backup log will be maintained to document the results of each Backup attempt.

1.5. Physical access controls must be implemented to protect physical Backup Copy media.

1.6. Backup Copies stored onsite must be stored in the computer room.

1.7. Backup Copies must be removed to a secure off-site location within 24 hours of creation with the exception of Backup Copies created on weekend days or statutory holidays.

1.8. The Backup Copy storage facility must be inspected at least once each quarter by the Director of IT Operations, or designate, and the results of the inspection documented in the offsite inspection log.

1.9. Recovery of Backup Copies must be tested semi-annually, at a minimum, and the results documented in the recovery verification log to ensure that Recovery is possible.

1.10. Tapes, media, tape drives, cleaning tapes, and other Backup media must be maintained according to the manufacturer's recommendations.

1.11. Backup tapes and other Backup media (excluding disk-to-disk Backup) must have, at a minimum, the following identifying information:

a system name,
a creation date, and
a Backup set name.

1.12. Backup Copies will be retained as follows:

Daily Backup Copies are retained for seven days;
Weekly Backup Copies are retained for five weeks;
Monthly Full Backup Copies are retained for 12 months; and
Annual Full Backup Copies are retained as required by the Records Management Policy.

2 TYPES OF BACKUPS

2.2. **Full Backup**: A Full Backup includes all files. This method ignores a file's Archive bit until after the Backup of the file is complete, at which point their Archive bits are turned off. Only one Full Backup will be done on a weekly basis.

2.3. **Incremental Backup**: Incremental Backups include only files that have been changed since the last Full Backup. This Backup executes daily and copies only files that have changed since either the last Full or Incremental Backup. The advantage of this method is quicker Backup requiring less downtime.

2.4. **Differential Backup**: A Differential Backup is a cumulative Backup of all changes made since the last Full Backup, that is, a Backup of the differences since the last Full Backup. The advantage to this is the quicker recovery time, requiring only a Full Backup and the last Differential Backup to restore the entire data repository.

Applicable Legislation and Regulations

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

Related References, Policies, Procedures and Forms

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

History

The Board of Governors Athabasca University, June 10, 2016(associated policy approved)