Athabasca University

PROCEDURE

Technology Infrastructure and Assets Lifecycle Procedure			
Parent Policy	Technology Management Policy		
Policy Sponsor	Vice President Information Technology and Chief Information Officer (VPIT & CIO)	**Category**	Administrative
Policy Contact	Deputy CIO	**Effective Date**	December 12, 2019
Procedure Contact	Deputy CIO	**Review Date**	December 12, 2024

1. Purpose

This procedure describes the University's approach to technology infrastructure management for its cloud infrastructure and its end-user device infrastructure. The approach aligns with the University's technology strategies and its technology architecture, including DevSecOps and test environments. The University also provides technology support for business applications and technology-enabled services.

2. Scope

The Deputy CIO is accountable for the effectiveness of all controls established to fulfill the requirements associated with all technology assets, services, solutions and changes including, but not limited to:

- Technology infrastructure including cloud infrastructure, cloud data storage, legacy physical and virtual infrastructure and data storage that is moving to the University Cloud, technology infrastructure that connects University office spaces to the Internet and infrastructure that is Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).
- Technology assets including end-user desktops, laptops, mobile devices, IoT devices, operating systems, digital signage, smart audio devices, virtual and augmented reality devices, and in-room and at-home communication technologies equipment.
- Software and applications, built or configured and integrated as software-as-a-service (SaaS).

3. Definitions

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*
Service Catalogue	A data set with information about all live IT Services, including those available for deployment.
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.
Technology Assets	End-user desktops, laptops, mobile devices, IoT (*Internet of Things*) devices, operating systems, digital signage, smart audio devices, virtual and augmented reality devices, and in-room and at-home communication technologies equipment.
Technology Infrastructure	Cloud infrastructure, cloud data storage, legacy physical and virtual infrastructure and data storage that is moving to the AU Cloud, technology infrastructure that connects AU office spaces to the Internet and infrastructure that is Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).
Technology Processes	Processes related to the acquisition, delivery, maintenance, replacement, and retirement of the University's information related technology.
Technology Services	Services provided by members of the University's IT organization to all students and employees pertaining to the acquisition, delivery, maintenance, replacement, and retirement of the University's information related technology.

4. Guiding Principles

4.1 Technology Management Policy standards associated with the technology infrastructure lifecycle procedure are:

a. Information Technology services must ensure that technology infrastructure components, including power and communications equipment, are managed in accordance with laws and regulations, technical and business requirements, vendor specifications, DevSecOps practices and health and safety guidelines.

4.2 All University technology infrastructure is budgeted for, provisioned, acquired, implemented, monitored and upgraded by IT.

a. The purchase of technology infrastructure by University units outside of IT is not permitted.

b. Technology infrastructure not secured and maintained by University IT is not permitted to access the University network.

4.3 All University technology assets are budgeted for, provisioned, acquired, implemented, monitored and upgraded by IT with the following exceptions:

a. In the case that an exception is granted by IT for the purchase of an end-user device that is not in the IT standard build choices, the cost of the exception device will be charged to the employee's unit.

b. Mobile phones purchased as for the employee's University work is charged to the employee's unit.

4.4 In accordance to AU's cloud-first strategy for security, accessibility and reliability, AU's technology infrastructure and data centre is in the cloud.

a. Cloud computing and cloud data storage will be tagged and provisioned to the employee's unit on request.

b. All legacy physical and virtual infrastructure computing and data storage must be migrated to the University cloud and physical equipment (servers, network components, network attached storage (NAS) drives, etc.) disconnected and recycled.

4.5 In accordance to the University's cloud-first strategy for security, accessibility and reliability, the University's technology assets, software and applications use cloud-enabled provisioning and updating, are hosted in the University cloud or are hosted in a partner's cloud instance.

a. All University end-user desktops and laptops provisioned by University IT will use cloud-based data backup, logging and update installation applications.

b. University's work productivity suite, including email, calendaring and video-conferencing functions is cloud-based.

c. As a cost-effective alternative to physical desktop or laptop, University IT provides a cloud-based virtual desktop that allows employees to log in securely to access a bundle of operating system, compute resources, storage space, and software applications.

4.6 University IT is accountable for the current University phone system infrastructure across University office locations in Alberta including the evolution of the current land-line infrastructure to a cloud-based VoIP PBX system and video-conferencing cloud-hosted model.

5. Applicable Legislation and Regulations

None applicable

5. Related Procedures/Documents

Digital Governance Control Framework - Governing Policy
Security of Digital Information and Assets Policy and related Procedures
Evergreening Procedure
Information Technology Change Management Procedure
IT Service Catalog
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)