Athabasca University

PROCEDURE

Operations Management 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 addresses lifecycle management of IT operations related to: baseline requirements; audit controls; project-related expectations; monitoring IT infrastructure; DevSecOps practices; and ongoing maintenance requirements.

2. Scope

The scope for the Operations Management Procedure includes:

- Technology Infrastructure
- Software and Applications

3. Definitions

Board Audit Committee	Assists the Board of Governors (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.
Change Advisory Board (CAB)	Includes IT personnel who have the authority to approve Operations Change Requests (OCR). CAB members have a clear understanding of the University's operational demands, the needs of the user community, and ICT environments.
Configuration Item	Any component that needs to be managed in order to deliver an IT Service including: • IT enabled business level services or functions

	• Information management elements (structured and unstructured IT assets) • Technology infrastructure templates and rules • Software and applications • Information and data privacy and security templates, rules and requirements and compliance evidence Operations, maintenance and recovery documentation
DevSecOps	The practice of building security into all aspects of the technology lifecycle and its assets into requirements, into design, into code, and into deployment, logging, and monitoring.
Digital Governance Committee	An advisory committee reporting to Executive Team for the purpose of assisting Executive Team in fulfilling its due diligence, fiduciary, financial reporting and audit response responsibilities by monitoring, evaluating and providing advice to the Executive Team on matters affecting all university digital initiatives.
Finance & Property Committee	Assists the Board in its oversight of the financial plans, policies, investments, practices, and performance of the University and approved capital projects, including information technology projects.
Lifecycle Management	In IT this model refers to how something is planned, managed and monitored from inception to completion, including evergreening.
Product Squad Owner	The Product Squad Owner is responsible to the business stakeholders for the product squad leadership of IT personnel providing initiation, transition and ongoing maintenance and support of a particular service.
Service Catalogue	A data set with information about all live IT Services, including those available for deployment.
Service Level Agreement (SLA):	An agreement between IT and a customer that describes the provision of an IT service, service level targets, and IT and customer responsibilities.
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	Athabasca University

4. Guiding Principles

4.1. Baseline requirements are required for University IT in maintaining current documentation of all University IT operations and services.

a. University IT will maintain the IT Service Catalogue of IT services provided to University students and employees.

b. The IT Service Catalog will contain a current list of Service Level Agreements (SLA) for the Service Catalog items, whether the SLA is between AU IT and units of the University or between a vendor provider and University IT.

c. Current documentation tracking all operating and capital major and minor digital initiatives is governed by the Digital Governance Committee

   i. Program and Project Managers and Business Analysts creating or overseeing the creation of project documentation, including but not limited to project proposals, business cases, charters, business requirements, functional requirements, technical requirements, timelines, project initiation forms, project change requests, work-in-progress reports and project/phase closure reports are required to follow the AU Project Management Framework that is governed by the Digital Governance Control Framework – Governing Policy.

   ii. Project documentation must be submitted for project controls oversight to the Digital Governance Committee.

d. Current documentation tracking implementation progress of external or internal audit recommendations is reported quarterly by the VPIT & CIO to the Board Audit Committee.

e. Current documentation tracking implementation progress of Integrated Resource Planning and Capital Planning initiatives is reported quarterly in the Digital Initiatives Progress Report by the VPIT & CIO to the Board Finance and Property Committee.

   i. The quarterly Digital Initiatives Progress Report is included monthly as a standing item in the Digital Governance Committee agenda package.

f. Current documentation tracking hours spent on all IT work and digital initiatives, including work on digital initiatives by non-IT employees, is captured in the Time Entry module of the University's ITM toolkit (ServiceNow).

i. Capacity, availability of resources and resource management is analyzed across the portfolio of digital initiatives using the ITM toolkit.

g. Current documentation of requests for IT support and services, including reports of outages are captured in the Service Desk module of the University's ITM toolkit (ServiceNow).

h. Current documentation of requests for moving products and services to AU's production environment are captured in the Change Advisory Board Standard Operating Procedure (SOP).

4.2. Controls will be applied through segregation of duties in members of the IT team and must be in line with the associated risk, security and audit requirements informed by the Enterprise Risk Management Framework, internal and external audit recommendations and the Information Security Program.

4.3. All IT-Related Projects must ensure the transfer of knowledge and skills to enable IT staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.

a. Create informative and understandable system maintenance and support documentation that is written in plain language and that is easily accessible, including service desk scenarios and electronic documentation.

b. Complete transition of all required project deliverables to ITM configuration items.

c. Involve IT staff in the creation of maintenance and support documentation, and integrate any procedures with existing operational procedures.

d. Provide training to IT staff on how to support the new system effectively. Include the business purpose of the system and service levels required.

e. Assess operations documentation, such as procedure manuals, online help, FAQs and help desk support material, for content and quality as part of user acceptance testing of the system.

f. Train IT personnel in operational procedures and related tasks for which they are responsible.

g. Ensure changes or new services promoted to the production environment have defined and documented the required operational procedures in advance of implementation, and establish during acceptance tests that they are complete, accurate and usable.

h. Collect regular feedback from IT staff on related non-IT employees on the adequacy of the operations documentation, procedures and related training.

4.4. IT Practices and SOPs will ensure the Change Advisory Board Procedure is integrated with the Project Management Framework and any recommendations from the Information Security Program so that the practice of DevSecOps can be utilized across all IT product squads.

4.5. Monitor the IT infrastructure and related events.

a. Implement steps for event logging based on best practices in security operations that identifies the information needed and ensures it is stored as per its retention requirements

b. Identify and maintain a list of infrastructure assets that need to be monitored, based on service criticality, and the relationship between configuration items (CIs) and the services that depend on the CIs.

c. Establish work instructions for monitoring event logs and conducting regular reviews.

i. Ensure that incident tickets are created in a timely manner when monitoring activities identify deviations.
ii. Ensure the Outage Incident Management SOPs are followed and, when warranted by severity, that the Outage Incident Management Report is signed off on by Deputy CIO and VPIT & CIO.
iii. Ensure the Security Incident Management SOPs are followed and, when warranted by severity, that the Security Incident Management Report is signed off on by CISO and VPIT & CIO.
iv. Ensure that sufficient chronological information is being stored in operations logs for audit purposes or to enable the reconstruction, review and examination of the time sequences of operations.

4.6. Undertake appropriate and timely maintenance including but not limited to:

a. Establish a preventive maintenance plan for all IT assets, considering cost-benefit analysis, vendor recommendations, risk of outage, the required number of qualified personnel and other relevant factors.

b. Review all activity logs on a regular basis to identify critical ITM asset components that require preventive maintenance. Update the maintenance plan accordingly.

c. Establish maintenance agreements involving third-party access to the Institution's ITM facilities for onsite and offsite activities, such as outsourcing.

d. Establish formal service contracts containing or referring to all necessary security conditions, including access authorization procedures, and procedures to ensure compliance with the Institution's security policies and standards.

e. In a timely manner, communicate to affected customers and users the expected impact of maintenance activities.

f. Incorporate planned downtime in an overall production schedule, and schedule maintenance activities to minimize the adverse impact on business processes.

5. Applicable Legislation and Regulations

None applicable

6. Related Procedures/Documents

Security of Digital Information and Assets Policy and related Procedures
Project Management Lifecycle Procedure
Evergreening Procedure
Digital Governance Control Framework – Governing Policy
AU Project Management Framework
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)