Digital Governance Control Framework – Governing Policy			
Policy Sponsor	Vice President Information Technology and Chief Information Officer (VPIT & CIO)	**Category**	Administrative
Policy Contact	VPIT & CIO	**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 technologies-based learning environment where learners of all ages and stages can seamlessly interact with learning experiences asynchronously or synchronously, online or offline, mobile and in-place. The Digital Governance Control Framework – Governing Policy sets out the underlying principles for all other IT policies and procedures to ensure Athabasca University identifies the right technologies to ensure reliability, security, stability and accessibility for Athabasca University students no matter how remote or rural their home or place of study is. These technologies allow Athabasca University to gain maximum value as well as develop and recruit the right talent to execute within its digital governance strategy. As a semi-virtual organization, we are committed to provide guidance to all those in the University Community who learn, work and create across multiple digital channels. In addition, there are four pillars relating to cybersecurity, automation, artificial intelligence and data ownership to underpin the Digital Governance Control Framework and its suite of policies and procedures.

Guidance to the University Community on the appropriate use of technologies is of particular importance in 2019 and beyond as technology has evolved and is continuing to rapidly evolve; affecting profound changes on us, data about ourselves, and how we work. Therefore, this control framework establishes key pillars related to four central areas of both technology growth and technology concern:

1. Cybersecurity - the need of Athabasca University to ensure that any technologies created, integrated or purchased are secure from tampering of any kind in any of their technology layers: network/transmission, storage/retrieval, application, user interfaces.
2. Automation - the need of Athabasca University to ensure that any technology automation used augments and enriches the university community experience.

3. Artificial Intelligence (AI) - the need of Athabasca University to ensure that AI created, integrated or purchased is used ethically, following the principles of the Montreal Declaration on Artificial Intelligence
4. Data ownership - the need of Athabasca University to maximize the personal ownership of data within the frameworks of employment and privacy laws.

These pillars relating to cybersecurity, automation, artificial intelligence and data ownership underpin the Digital Governance Framework's guiding principles and its suite of policies and procedures.

2. Scope

This control framework serves as the governing document and is the overarching policy for all of the related IT policies and procedures. It applies to the governance and management of the University's information and related technology assets, processes and services. Digital governance safeguards the University in fulfilling its cybersecurity, due diligence, fiduciary, financial reporting and audit response responsibilities. The VPIT & CIO, supported by the IT reporting line, leads creation, integration, evaluation and ongoing sustainability of all digital/technology operational initiatives in support of the University's strategic plan. The VPIT & CIO will advise the University Community regarding continuance of or amendments to such standards and procedures as may be required. The scope of the Digital Governance Framework and the policies and procedures contained within it apply to employees of University Community.

3. Definitions

Terms used as defined in the IT-Specific Glossary	Refer to IT-Specific Glossary in Appendix A

4. Guiding Principles

4.1. Vision

a. Athabasca University envisions a campus where the very best of open and proprietary tools ensure better learning outcomes for our students and better learning creation capabilities for our employees.

b. Attract and retain diverse talent who share a passion for empowering learners everywhere by creatively integrating the best of mobile and accessible learning tools and platforms.

c. Information Technology staff will participate in, encourage and support a culture of lifelong learning and digital entrepreneurship.

4.2. Digital Governance Control Framework

A suite of policies and procedures enable the University to manage both information and related technology through governance structures and processes that:

a. Support the University's strategic direction and mandate to achieve positive outcomes.

b. Communicate information and related technology directions.

c. Collaborate with the University Community stakeholders (including students and employees) to align with their informed needs and ensure mutually informed decisions are made.

d. Optimize the return on investments made in information and related technology assets.

e. Deliver quality services in support of University objectives.

f. Provide assurance that IT controls are implemented, reviewed, monitored and evaluated.

g. Manage IT risk, including cybersecurity and information security across all University business areas to protecting digital information and risk-free use of IT Assets.

h. Ensure responsibilities and accountabilities are assigned, understood and accepted.

i. Comply with legislation, regulations and contractual requirements.

4.3. Integration and Interoperability

a. Integration of all aspects of the learning experience ecosystem of the future will be a priority for the VPIT & CIO, including ensuring learner data is secure, governed and follows best practices in data integrity and the four pillars above.

b. Provision of a digital learning environment envisioned by the Learning Framework that allows students to learn about their personal education journey over their lifetime and allows our employees to understand and continuously improve digital learning at scale across all learning experiences in the environment.

c. Optimize the inclusiveness and communication of IT product development and enhancement plans and priorities through the governance process to

ensure IT plans are understood by the University Community as a key member of integrated planning and continuous improvement.

4.4. Enterprise Approaches

a. Combine the best solutions with an ecosystem of digital technology specialists in media-rich learning productions, virtual reality, augmented reality and artificial intelligence to build and continuously improve the digital learning environment of the future.

b. Ensure the IT architecture provides security, stability and growth opportunities for Athabasca University's digital innovations and those of our partner universities and colleges.

c. Standardize by establishing and implementing with leadership across the university, an organization-wide Data Governance Framework to improve data ownership, accountability, quality, integrity, and to mitigate data-related risks.

d. Remove artificial distinction between enterprise and divisional systems and evolve IT governance to a university-wide Digital Governance Committee that supports the Integrated Resource Planning Framework, creating collaboration, fiscal accountability, transparency and flexibility to innovate for all university digital needs.

4.5. Best Practices

a. We will expand and enrich Lean governance and management practices in a commitment to openness, transparency, clarity and to minimize bureaucracy.

b. Embed prioritization across digital systems implementations, enhancements and upgrades for regular review and voting within the expanded Digital Governance Committee model.

c. Conduct annual reviews of the University's adopted IT Lean portfolio strategy and governance frameworks to ensure their effectiveness.

d. Once new strategies and processes are well-established via the governance process, implement review and compliance procedures to ensure quality of software design, code, and supporting cloud infrastructure are consistent as enterprise solutions.

5. Applicable Legislation and Regulations

Freedom of Information and Protection of Privacy Act
Canadian Anti-Spam Legislation (CASL)
European Union General Data Protection Regulation (GDPR)

6. Related Procedures/Documents

Configuration Management Procedure
Investment Portfolio Management Procedure
Project Management Lifecycle Procedure
Information Technology Risk Management Procedure
Digital Enterprise Architecture Policy
Security of Digital Information and Assets Policy and related Procedures
Information and Data Management Policy and related Procedures
Technology Management Policy and related Procedures
Information Technology Service Orientation Policy and related Procedures
Montreal Declaration on Artificial Intelligence
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)

APPENDIX A: IT-SPECIFIC GLOSSARY	
Account	A means for accessing IT 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.
Agile Methodology (IT)	Enterprise Architecture development that is achieved by supporting practices that are business-outcome-driven, customer-centric, collaborative and cooperative, as well as with continual stakeholder feedback.
Application	A software program that collects, manipulates, processes, stores, distributes, displays or prints Digital Information or Content.
Approval Authority	Governing body or position with authority (or delegated authority) to approve a policy within this Policy Framework.
Archive	The relocation of Digital Information to the AU cloud for long-term storage when such information does not need to be readily accessible, but may be needed in the future.
Asset Owner (IT)	University employee or member of Managed Security Services partner personnel to whom the Vice-President IT and CIO or CISO has delegated the authority to grant access to an IT Asset.
Authentication	A means of verifying the identity if an Authorized User, including by two-factor identity verification.
Authorized User	A person who has been granted access to an account and whom access has not been rescinded or terminated.
Backup	The copying of Digital Information from one electronic medium to another.
Backup Copy	The copy of Digital Information made during Backup.
Backup and Recovery Testing	Conducted to demonstrate that backup and recovery procedures are effective. It is a best practice to test these in a test environment.
Board	The Governors of Athabasca University
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

APPENDIX A: IT-SPECIFIC GLOSSARY	
	financial reporting and accounting control policies and practices of the University.
Board Policy	Board Policy provides governance and accountability, and pertains to strategic positioning, risk management, fiduciary responsibility and legislative compliance.
Business Architecture	Focuses on a common, enterprise-level business language and framework for documenting how the business is structured to support a technology strategy within a business strategy.
Business Architecture (Methods and Processes)	Strategic and tactical use of business architecture methods and tools, including but not limited to business process engineering, business process management, business process modelling, workflow, and similar technology in relation to business capabilities and design. Best practices for integrating business processes that span multiple internal organizations.
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.
Change Request or Request for Change (RFC)	The objective of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes in order to minimize the impact of change-related incidents and to improve day-to-day operations.
Confidential Digital Information	Information identified as confidential or Protected B Classification as per the Data Classification procedure of the Information Management Policy.
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
Configuration Management	The process responsible for maintaining information about configuration items required to deliver an IT Service, including their

APPENDIX A: IT-SPECIFIC GLOSSARY	
	relationships. This information is managed throughout the life cycle of configuration items.
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.
(Significant) Cyber Security Incident	An incident which has one or more of the following characteristics will be considered significant: • Has a medium to high impact on the standard operation of services within the University; • May be a breach or violation of policy or standards and; • May occur inadvertently or deliberately
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.
Data Architecture	Overall structure of data and data-related resources as an integral part of the enterprise architecture. Related terms: Data Architect.
Data Custodian	Responsible for the technical environment and database structure necessary to ensure safe custody, transport and, storage of data. Development and implementation of business rules may be done in collaboration with business areas and their data stewards.
Data Governance (DG)	Data governance (DG) refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures, and a plan to execute those procedures. The initial step in the implementation of a data governance program involves defining the owners or custodians of the data assets in the enterprise. A policy must be developed that specifies who is accountable for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness, and updating.

APPENDIX A: IT-SPECIFIC GLOSSARY	
	Processes must be defined concerning how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack. A set of standards and procedures must be developed that defines how the data is to be used by authorized personnel. Finally, a set of controls and audit procedures must be put into place that ensures ongoing compliance with government regulations. See also: Data Custodians, Data Stewards.
Data Lifecycle Management	Data lifecycle management is the process of managing business information throughout its lifecycle, from requirements through retirement. The lifecycle crosses different application systems, databases and storage media.
Data Management	Data management is the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. Activities comprise data policies, data planning, data element standardization, information management control, data synchronization, data sharing, and database development, including practices and projects that acquire, control, protect, deliver and enhance the value of data and information.
Data Quality	While there is no universal definition for Data Quality, Statistics Canada defines it as the quality of information in terms of its fitness for use. This is a multidimensional concept embracing both the relevance of information to users' needs, and characteristics of the information such as accuracy, timeliness, accessibility, interpretability and coherence that affect how it can be used.
Data Sharing	The transfer of data between different organizations, branches or departments to achieve an improvement in the efficiency and effectiveness of public service delivery.
Data Steward	A subject matter expert who is designated by an executive role. This role has operational responsibility for data and information files in the business domain including: the identification of operational and business intelligence data requirements within an assigned subject area; the quality of data and information, business definitions, data integrity rules, compliance with regulatory requirements and conformance to information/data policies and procedures; application of appropriate security and access controls; and identifying and resolving related issues.

APPENDIX A: IT-SPECIFIC GLOSSARY	
Data Stewardship	The business/operation area accountable for the data set. Business areas responsible for data stewardship within the University include: e.g. Research Data (Research), Systems data such as Learning Engagement Data, Student Records and Operational Data (IT), Privacy and Records Management (Governance), Archives and Learning Resources (Libraries), Personnel Records (HR), Financial Records (Finance).
Data Validation	The process of data cleansing to ensure data quality.
Development Environment	A controlled environment where application, IT services, and other builds are assembled prior to moving into test or production environments.
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 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.
Digital Governance Technical Sub-Committee	A non-voting working group who reports to the Digital Governance Committee (DGC). The purpose of the sub-committee is to facilitate the successful delivery of the technical and security-related aspects of approved digital initiatives.
Digital Information or Content	Binary encoded information.
Digital Initiatives	Major strategic or operational IT projects, digital in nature, that result in the creation or acquisition of a tangible capital asset (e.g., system, hardware), or that extend the useful life of an existing capital asset excluding internally or externally funded research projects.
Digital Storage Device	A device that can retain binary encoded information in a permanent
End-User Device	A computing device used by End-Users including desktop computers, net stations, laptops, and mobile devices (e.g., tablets, smart phones), monitors headphones and webcams.

APPENDIX A: IT-SPECIFIC GLOSSARY	
Enterprise Architecture	A means of aligning and understanding the relationships and interdependencies between an organization's business processes and its technological environment(s).
Evergreening	The process of ensuring Technology and Digital Assets remain current and are replaced or retired on a regular schedule. An Evergreening strategy also ensures that the risks associated from running legacy end-user devices (and their operating Systems) are mitigated, and that the costs to mitigate these risks can be planned and distributed over multiple fiscal years.
Executive Team	Is comprised of the President; Provost and Vice-President Academic; Vice-President, Finance and Administration and Chief Financial Officer; Vice-President, Information Technology and Chief Information Officer; Vice-President, University Relations; University Secretary; Chief Human Resource Officer; the Chief of Staff, Office of the President, and any other position as so designated.
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.
FOIP	*Alberta Freedom of Information and Protection of Privacy Act* R.S.A. 2000, c. F-25, as amended from time to time.
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 VPIT&CIO.
Guideline	Suggested approaches, best practices and/or additional information related to procedures.
"I-Care" Values	Reflects the University of Athabasca's commitment to values characterized by integrity, community, adaptability, respect and excellence.
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

APPENDIX A: IT-SPECIFIC GLOSSARY	
	Information, etc.) owned by, under the custody of, or commercially made available to, the University.
Identity Management	The set of policies, procedures and standard operating procedures (SOPs) for ensuring that the proper people in the University community have the appropriate access to technology resources. Identity Management systems fall under the overarching umbrella of IT security and Data Management.
Identity Verification (Two-Factor)	Involves user identifying into an Athabasca University system using their login ID and password and then having a second form of authentication for validation (numerical code texted to mobile phone, email to secondary email address, touch ID, facial recognition, etc.) to prevent use of account based on a stolen password.
Incident (IT)	Any failure or malfunction of IT Assets that results in a loss of Service to the University community.
Incident Manager	An IT employee or member of the Managed Security Services personnel designated to assign personnel to, coordinate the response to, and issue a report regarding an ICT Security Incident or ICT Incident.
Information Architecture	Focuses on the management of information resources including storage, retrieval, delivery, classification and utilization of information to best deliver shareholder values as well as to support technology strategy.
Information/Data Asset	Includes all data, information and intellectual property.
Information and Data Security Classification Levels	Security levels that will be used to classify all data and information that are received, created, held by or retained on behalf of the University. Typical classifications are public and protected (e.g., need to know, confidential and restricted).
Information Management	Information management involves the planning, directing and controlling of all of the University's IT assets to meet corporate goals and to deliver programs and services. Information management refers to the application of consistent practices related to planning, creation, capture or collection, organization, use, accessibility, dissemination, storage, protection and disposition (either destruction or permanent retention) of information.

APPENDIX A: IT-SPECIFIC GLOSSARY	
Infrastructure Architecture	Focuses on the hybrid cloud and on-premise operations, network engineering, server sizing, storage management, backup &restore technologies, disaster recovery and cloud architecture design.
Investment Classification – Major IT Investment	Large or major IT investments including strategic, mission-critical, high-risk, complex, major new system/service, or major upgrade.
Investment Classification – Minor IT Investment	Operational low to medium risk, uncomplicated, minor change(s) to existing system/service.
Legislation	Applicable law that is enacted by the Federal Government, Provincial Legislature, Municipal Council, or other governing body having jurisdiction.
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.
Log-In Management	The process of recording and storing accesses to accounts for auditing and security management purposes. Also known as logging.
Member	Member of the University Community.
Metadata	Structured information about data. Metadata describes, defines, explains, locates, and otherwise makes it easier to retrieve and use an information resource or data asset. Metadata is essential to the way in which the data or information is used.
Phased Delivery	Dividing the deliverables of a large digital initiative or project into bundles that are delivered via a series of sequenced project phases.
Policy	A published statement that reflects the University's strategic direction, governing principles and institutional goals. Policies are statements of expectation, conduct or outcome that comply with relevant legislation, regulation and institutional requirements. Policy normally does not include operational procedure, except in very specific circumstances where policy and procedure cannot be appropriately separated.
Policy Contact	The individual who has responsibility for operationalizing the policy and/or procedure.

APPENDIX A: IT-SPECIFIC GLOSSARY	
Policy Coordinator	The designated individual in the Office of the University Secretariat, who provides planning, co-ordination and facilitation support for the policy sponsor in the development and maintenance of policies and procedures.
Policy Sponsor	The executive officer or director of the department, centre or office who is responsible for the implementation of policies and procedures and is accountable for ensuring staff compliance with established policies and procedures. If the executive officer or director delegates the implementation of the policies and procedures to another person, a written delegation will be kept on file in the working policy file with the Office of the University Secretariat.
Privileged Account	An account that is authorized to a user who is trusted to perform security-relevant functions that ordinary users are not authorized to perform. The Authorized User of a Privileged Account also has the ability to control the access or permissions of other Authorized Users.
Portfolio Management	Collection of projects or programs and other work that are grouped together to facilitate effective management of that work to meet the University's strategic objectives.
Procedure	The established operational steps to be followed in order to ensure that the outcomes and values expressed in legislation, collective agreements or a policy are achieved.
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.
Program	(As it relates to IT project management) A group of related projects that are managed in a coordinated way to obtain benefits not available from managing them individually.
Project	A temporary endeavor undertaken to create a (unique) product, service or result.
Project Management Committee (IT)	Advisory Body who steers a digital project's delivery from its start to the finish to ensure the project remains focused on delivery of defined business outcomes.
Project Management Framework (PMF):	AU's adopted project management methodology that guides the delivery of a project once it has been initiated.

APPENDIX A: IT-SPECIFIC GLOSSARY	
Protected Information	Information that is protected as per the Data Classification procedure of the Information Management Policy.
Records Management	The application of systematic control to recorded information that is required for the administration and operation of the University.
Records Retention and Disposition Schedules	An established timetable for maintaining University records, and their ultimate destruction or preservation.
Recovery	The restoration of point-in-time copies of Digital Information from a Backup Copy.
Responder	An IT employee or member of the Managed Security Services personnel assigned by the Incident Manager to investigate an IT Security Incident or IT Incident.
Risk Management	The responsible administration of any digital initiative requires awareness of risks that can occur with uncertain frequency and impact and create challenges in meeting strategic goals and objectives. Handling such risks, through a risk management approach, is essential to achieving objectives. Appropriate risk management ensures all new or known risk attributes have been defined (e.g., owner, likelihood, impact) and analyzed and alerting the PSC to risk changes and their potential impact to the project, other projects, or the organization.
Risk Register	A document that identifies the potential risks to a digital initiative along with attributes for each risk.
Risk Tolerance (IT)	Depending on risk type, defined by either Deputy CIO, CISO or Privacy Officer, as the acceptable level of variation relative to the achievement of objectives.
Security Incident Report (IT)	A written report using the approved IT Security Incident Report Form.
Security Incident (IT)	A digital security incident is indicated by a single or a series of unwanted or unexpected information security events that present a significant risk to the 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.

APPENDIX A: IT-SPECIFIC GLOSSARY	
	• 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 Act or activities Technology involving IT Assets.
Sensitive Data and Information (Identity)	Sensitive data is associated with a person and is typically identifying. Any data or information that reveals: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; and data concerning health or a natural person's sex life and/or sexual orientation.
Service	A means of delivering value to stakeholder(s) by facilitating outcomes the stakeholder wants to achieve.
Service Catalogue	A data set with information about all live IT Services, including those available for deployment.
Service Change	Describes IT Service, documents service level targets and specific responsibilities of IT Service providers and their stakeholders.
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.
Service Level Management	Service Level Management is the process responsible for negotiating service level agreements (SLAs), ensuring the SLAs are met, and ensuring that all IT service management processes, operational level agreements and underpinning contracts are appropriate for the agreed service level targets. This process further monitors and reports on service levels and holds regular stakeholder reviews.
Service Management	Service Management is a set of specialized organizational capabilities for providing value to stakeholders in the form of service.
Significant Cyber Security Incident	An incident which has one or more of the following characteristics: • Has a medium to high impact on the standard operation of services within the University;

APPENDIX A: IT-SPECIFIC GLOSSARY	
	• May be a breach or violation of policy or standards and; • May occur inadvertently or deliberately.
Software Architecture	Focuses on delivering and developing technology strategy related to software and solution implementation.
Solution Architecture	Focuses on delivering full architectural solution based on the inputs from Business/Information/Software/Infrastructure Architecture and is the realized through implementation by Project Portfolio Management of one-time projects or ongoing, continuous improvement initiatives.
Standard	A mandatory requirement, code of practice or specification.
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.
Student	Any individuals enrolled in Athabasca University courses who are in or on Athabasca University facilities.
Supervisor	A person who has charge of a work site or authority over a worker.
System Administrator	Personnel who are responsible for the upkeep, configuration and reliable operation of specific ICT Assets.
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.

APPENDIX A: IT-SPECIFIC GLOSSARY	
Test Environment	A controlled environment used to test configuration item, builds, IT Services, processes, etc. in order to verify these meet specification or agreed upon requirement.
University	Athabasca University
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.
User ID	A unique identifier assigned to an Authorized or Service to enable access to IT Assets.
User Interface	The means by which an End-user interacts with a Website, Web Page, Digital Content, learning management system or Application (including Mobile Applications) through End-user Devices, both hardware (e.g., keyboard, mouse, remote control) and software (e.g., menus, toolbars, windows, buttons).
Vendor	A supplier of Goods and Services
VPIT and CIO	Vice-President Information Technology and Chief Information Officer of the University