IT GOVERNANCE & TECHNOLOGY MANAGEMENT

This document is the parent policy for any College procedures. Questions regarding this policy are to be directed to the identified Policy Owner.

Category:	E. Information & Technology Management
Policy Number:	E01
Approval Date:	January 26, 2024
Effective Date:	January 26, 2024
Policy Owner:	Vice President, Student Experience Director, Information Technology

Objective:

Technology is a key enabler to achieving well-managed information. Therefore, it is critical to manage both information and technology through governance structures and processes that:

1. Support the strategic direction and mandate of Olds College of Agriculture & Technology (the "College") to achieve positive outcomes.
2. Communicate information and related technology directions.
3. Collaborate with information users to align with their needs and ensure mutually informed decisions are made.
4. Optimize the return on investments made in information and related technology assets.
5. Comply with legislation, regulations and contractual requirements.
6. Provide assurance that controls are implemented, reviewed, monitored and evaluated.
7. Manage risk throughout the institution.
8. Ensure responsibilities and accountabilities are assigned, understood and accepted.
9. Maintain an adequate complement of resources to achieve the strategic direction and mandate.
10. Ensure the information users are appropriately educated and trained.

The preservation of confidentiality, integrity, and availability of systems and digital information utilized by the College constituents is critical. This policy supports the secure operation and use of the College's digital assets, systems, and by extension, the overall objectives. This policy defines the responsibility to:

1. Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.
2. Manage the risk of security exposure or compromise.
3. Assure a secure and stable information technology (IT) environment.
4. Identify and respond to events involving information asset misuse, loss or unauthorized disclosure.
5. Monitor systems for anomalies that might indicate compromise.

	6. Ensure overall management process that includes the planning, implementation, maintenance, review, and improvement of information security. 7. Promote and increase the awareness of information security. How the College protects digital information and systems has a direct impact on the College's reputational risk. Effective Enterprise Architecture is achieved through the application of a comprehensive and thorough process for describing current and future structure and behaviour for the College's processes, information, applications, technology and supporting the people portfolio. It creates a shared vision for the College's information and digital capabilities by ensuring: 1. Organizational needs drive digital, information and related technology strategies and plans. 2. An adaptive and agile response to business requirements. 3. The architectures work together efficiently and effectively to provide consistent services, accessible information, scalable solutions and flexible technology. 4. Seamless integration of applications with business processes. 5. Analysis of current resources and their use to identify opportunities for cost savings and continuous improvement. The planning and budget processes are supported by directly linking digital investments to the accomplishment of the College's strategies and College Leadership Team (CLT) School/Area Operational Priorities Planning process.
Policy:	The College will manage its information and technology assets and services through effective governance structures and processes that provide leadership, accountability and transparency and engage key stakeholders to support the achievement of positive outcomes and facilitate implementation of strategic oversight and decision making. The College will provide a risk-based digital security approach, resulting in the careful management of college security controls. To provide direction related to digital security, the College has created a framework of digital security standards, procedures, guidance and baselines. The College adheres to an Enterprise Architecture framework and principles that maximizes the digital capabilities of the College and aligns with provincial initiatives and the College's strategies and mandates. The Enterprise Architecture approach complies with legislation and oversight requirements of the College: 1. At the College, Enterprise Architecture is a business strategy which captures, documents, classifies and analyzes all aspects of the enterprise in order to make the information relevant for decision makers, including leaders, business analysts and technology specialists.
Scope:	All employees or third parties associated with the College must adhere to this policy as it applies to the digital information controlled by the College; all digital assets owned, leased and managed by the College; and all services provided by the College, both internally and to clients.
Definitions:	**Digital Asset:** A collection of non-tangible binary data stored in an electronic format that is self-contained, uniquely identifiable, and has value to the institution. Examples include (but are not limited to) images, photos, videos, files containing text, spreadsheets, slide decks, contact lists, electronic notes, e-mail, databases, logs, etc.

OLDS COLLEGE
OF AGRICULTURE & TECHNOLOGY

	Application Architecture: A structural map of how an organization's software applications are assembled and how those applications interact with each other to meet business or user requirements. **Business Architecture:** Represents holistic, multidimensional business views of capabilities, end-to-end value delivery, information, and organizational structure; and the relationships among these business views and strategies, products, policies, initiatives, and stakeholders. **Information Architecture:** Defines an organization's business information assets, as well as the assets' sources, structure, classification, and associations. Information Architecture enables understanding and utilizing enterprise data and analytic assets to achieve desired business outcomes. **Information Security Architecture:** Describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans. **Technology Architecture:** Describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc.
Related Information:	IT Technical Frameworks, Standards & Protocols
Related Procedures:	E01 IT Governance & Technology Management Procedure E01 Digital Security Procedure E01 IT Enterprise Architecture Procedure
Review Period:	3 years
Revision History:	New: October 1997 Revised: June 2013 Revised: May 2020 Revised: January 2024