IT ENTERPRISE ARCHITECTURE

This procedure is governed by its parent policy. Questions regarding this procedure are to be directed to the identified Procedure Owner.

Category:	C. Campus Development
Parent Policy:	C04
Approval Date:	December 9, 2025
Effective Date:	December 9, 2025
Procedure Owner:	Director, Information Technology

Overview:

This procedure encompasses the following individual domains that form Enterprise Architecture:

1. Business Architecture
2. Data Architecture
3. Application Architecture
4. Technology Architecture
5. Information Security Architecture

Procedures:

The Enterprise Architecture principles will guide the selection, design and implementation of business solutions for the following three aspects of information, applications and technology. All principles are interrelated and collectively applied to:

1. provide a framework within which Olds College of Agriculture & Technology (the "College") makes informed and considered decisions about Digital Solutions and Information Technologies.
2. establish evaluation criteria for the selection of products or product architectures.
3. define the functional requirements of Enterprise Architecture.
4. assess existing digital solutions, IT systems and the future strategic portfolio for compliance with the defined architectures.
5. support governance activities related to the College's Enterprise Architecture.

Business Architecture Principles

The following principles apply to Business Architecture:

1. Effectively addressing college business and operational needs is the basis for business architecture decision making.
2. Decisions are made with the intention of achieving maximum benefit to the College.
3. Applications are developed for use across the enterprise in preference to similar or duplicative applications which are used in a particular department, where possible.
4. Enterprise Resource Planning (ERP) capabilities will be delivered through a

common, integrated platform rather than disparate, standalone applications, where possible.

Data Architecture Principles

The following principles apply to Information Architecture:

1. Information is a valued corporate asset and is managed accordingly.
2. Recognizing staff time is a valuable institutional resource, data architecture takes into account the user experience in architecture decision making.
3. Data is accessible and shared across departments for users to perform their functions.
4. Each data element has an Information Data Custodian accountable for data quality.
5. Data is defined consistently across the College and the definitions are understandable and available to all users.
6. Information is protected from unauthorized use and disclosure.
7. Information is verified for data integrity and validity.

Application Architecture Principles

The following principles apply to Application Architecture:

1. Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.
2. Applications are easy to use and the underlying technology is transparent to users so they can concentrate on tasks at hand.
3. Cloud-based Software as a Service (SaaS) solutions will be prioritized to ensure business resilience and enhance cybersecurity. On-premise applications will be deployed only by exception when they provide a unique and critical capability not available in the cloud.

Technology Architecture Principles

The following principles apply to Technology Architecture:

1. Changes to applications and technology are only made in response to specific business needs and requirements.
2. Changes to the enterprise information environment are planned and implemented in a timely manner.
3. Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.
4. Technology will be centrally managed by the IT department to maximize:
    a. strategic oversight,
    b. streamlined operations,
    c. workplace effectiveness,
    d. financial sustainability,
    e. compliance with IT security practices,
    f. effective segregation of duties practices,
    g. system knowledge succession.
5. Enterprise operations are designed with sufficient resiliency to ensure a high probability of continued operations.
6. Software and hardware conforms to defined standards that promote interoperability for data, applications and technology.

Information Security Architecture Principles

The following principles apply to Information Security Architecture:

1. Systems and digital solutions are in compliance with the Digital Security

	Procedure and associated standards. 2. Systems must integrate with the College's endorsed identity management system and single sign-on (including multi-factor authentication) solution wherever possible. Generally, the College will endeavour to provide intuitive and seamless user experiences on all online systems. Systems are designed to be simple to use, effective and as automated as possible.
Definitions:	**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, multi-dimensional 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. **Data Architecture:** Defines an organization's business information assets, as well as the assets' sources, structure, classification, and associations. Information architecture enables understanding and utilizes 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. **Information Data Custodian:** This responsibility sits with specific Information Technology Department designates. Data custodians are responsible for safe custody, transport, storage of the data and implementation of associated business rules.
Related Information:	C04 IT Governance & Technology Management Policy C04 IT Governance & Technology Management Procedure C04 Institutional Data Governance Procedure C04 Digital Security Procedure IT Technical, Standards & Protocols 1. STANDARD - IT Service Continuity 2. STANDARD - Backup and Recovery a. PROTOCOL - Backup and Recovery Protocol 3. Olds College IT Service Recovery Plan 4. STANDARD - Cloud Services
Review Period:	3 years
Revision History:	New: April 2015 Revised: November 2023 Revised: December 2025