DIGITAL SECURITY

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

Category:	E. Information & Technology Management
Parent Policy:	E01
Approval Date:	November 30, 2023
Effective Date:	November 30, 2023
Procedure Owner:	Director, Information Technology

Overview:

Digital security does not happen by accident; rather, it must be strategically designed to ensure that all the appropriate aspects are covered. This Digital Security Procedure, in concert with the IT Governance & Technology Management Policy, describes the mechanism by which the policy is to be realized.

By its very detailed nature, Digital Security requires precise components to guide its operations as identified by well known IT Governance models. This Digital Security Procedure illustrates the creation of a set of IT specific Standards & Procedures to frame the development of the Digital security program at Olds College of Agriculture & Technology (the "College").

Procedures:

The following are the Digital Security components that support the confidentiality, integrity and availability of the College digital data. These statements align with broadly accepted security practice and Digital Security Governance models relating to the following eight Digital Security categories:

1. Governance & Compliance
    a. The Director, Information Technology, in consultation with others within the IT Department, shall oversee the Digital Security program and ensure that it is adequately enforced, regularly maintained and monitored for compliance and efficacy.
    b. All information, such as contact lists, files, folders, email attachments and emails, sent or received on the College email systems are proprietary to the College and therefore considered to be institution property for records retention, legal and digital security purposes.
    c. For the purposes of securing the College data in its various states, a Security Data Classification mechanism will be implemented that categorizes the College data into groups of like sensitivity.

2. Policy, Standards, Guidelines & Procedures
    a. Digital Security Standards, Procedures and other relevant security instruments are developed to support the overall intent of the IT Governance & Technology Management Policy.

3. Security Architecture
   a. Cryptographic technologies employed by the College will support good practices for cryptographic key management including the ability to generate, change, revoke, destroy, distribute, certify, store, use and archive cryptographic keys.
   b. The College digital data will be disposed of in a manner that is appropriate for its level of sensitivity.
   c. Internet facing applications will be protected utilizing a layered approach to security treatments.
   d. Secure coding practices will be established and enforced for all application development.
   e. Suitable IT Standards, Procedures, baselines, and technological controls must be in place to ensure the security of the network environment, digital data and the protection of the security technologies utilized.
   f. Automated malware detection, prevention and correction mechanisms will be operated, monitored and maintained on all appropriate institution endpoints with access to digital information.
   g. Where, due to the sensitivity of the data involved, or the mobility of the device, a cryptographic mechanism is to be deployed and centrally managed that encrypts all data stored on the device.
   h. User Accounts/IDs granted access to resources on the College network will be unique, authorized, authenticated and managed through the creation of IT Security Standards and Procedures governing the authorization, creation, amendment, suspension, removal and review of accounts/access privileges.
   i. File shares/folder access will be carefully controlled and monitored ensuring that only authorized personnel may have access to stored information.
   j. Passwords will be of appropriate length and complexity.
   k. Remote access to the College Information Technology resources shall be permitted only through IT approved remote access methods.
   l. Physical access to core IT devices will be secured such that only those requiring physical access to the devices as part of their normal employment function are granted access.

4. Risk & Change Management
   a. A Quantitative Risk Assessment Methodology will guide the application of IT Security controls throughout the College environment.
   b. Known or identified IT risks will be tracked, rated and items identified to be above the organization's risk appetite will be targeted for remediation to lower the risk to an acceptable level.
   c. An IT security specialist will be an integral member of the Change Advisory Group, to help ensure that IT changes to the College environment do not introduce unacceptable levels of risk.

5. New Projects Participation
   a. An IT security specialist will contribute on all new IT projects to allow for appropriate security measures to be designed into new solutions from the beginning and ensure that College’s Digital Security Standards are met.

6. Monitoring, Assessing & Reporting
    a. All devices that are, or have connected to, the College network are subject to monitoring and/or auditing.
    b. Regular Digital Security testing and/or risk assessments will be performed to ensure compliance with established standards and baselines and to help minimize exposure to security risk due to changes within the environment, advancements in detection capabilities or newly identified threats to the organization.
    c. Metrics, suitable to demonstrate the efficacy of the overall Digital Security Program will be developed, maintained and reported to senior management.
7. Security Incident Response, Investigations & Forensics
    a. A Security Incident Response Team (SIRT) will be established and will be responsible for the creation and enablement of a SIRT Process to investigate, analyze, contain, eradicate, recover and learn from digital security events.
8. Security Training & Awareness
    a. A regular mandatory Digital Security training program will be administered and tracked which includes anyone with access to the College digital information.
    b. The provision of occasional Digital Security Awareness for the College staff/faculty will be developed and offered to increase digital security awareness of the institution.
    c. The process to enable these Policies is presented in the IT Governance & Technology Management Procedure which outlines the identified approach.

The Digital Security Procedure establishes executive support for the creation of the IT Security Standards, Procedures and other instruments required to build and maintain a comprehensive security program.

An IT Security Advisory Working Group, will serve to provide general feedback on the broader IT Security Standards and other relevant instruments. The IT Security Advisory Working Group may include ad-hoc representation from IT, Staff, Faculty, People & Culture, and/or Procurement.

Current disparities from the IT Security Standards will be determined and analyzed, with relevant solutions being implemented to ensure all aspects of information technology governed under this procedure are in alignment with the implemented security standards.

The Director, Information Technology, will be responsible to validate alignment with the approved Standards. In cases where there is incongruence, the issue(s) will be rectified as soon as possible.

Exceptions:

A request for exception to this policy must be submitted for approval to the Director, Information Technology, who will then make a recommendation to the IT Security Advisory Working Group for a final decision, by following the process as described in the Digital Security Exception Request Protocol. Exceptions will be granted for up to one year and will be reviewed annually at which time the exception may be revoked, revalidated or extended for up to another one-year term. The documented exceptions will be maintained by IT.

Definitions:

Policy: A statement that defines a course or principle of action adopted or proposed by the institution.

	IT Security Standard: A set of like-directives used as a measure, norm, or model to achieve a specified level of compliance. **IT Security Procedure:** A series of IT specific actions or steps taken by specific actors in order to achieve a precise IT Security objective. **IT Security Advisory Working Group**: Ad-hoc body from across the college including both academic and administrative areas. **IT Security Baseline:** A specific deployment / implementation guideline, explicit to a technology, usually a software or hardware build (e.g. the following services will be disabled on a Windows 2019 Server…etc.) which dictates security configuration settings.
Related Information:	E01 - IT Governance & Technology Management Policy E01 - IT Governance & Technology Management Procedure E01 - IT Enterprise Architecture Procedure IT Technical Standards & Protocols 1. STANDARD - Acceptable Use 2. STANDARD - Account Lockout 3. STANDARD - Data Classification 4. STANDARD - Data Retention 5. STANDARD - Data Encryption 6. STANDARD - Data Transmission 7. STANDARD - Database Security 8. STANDARD - Electronic Media Disposal 9. STANDARD - IT Change Management a. PROTOCOL - IT Change Management 10. STANDARD - Logging/Monitoring 11. STANDARD - Patch & Vulnerability Management a. PROTOCOL - Vulnerability Management 12. STANDARD - Cryptographic Key Management 13. STANDARD - Malicious Software Prevention-Detection-Eradication 14. STANDARD - Mobile Device 15. STANDARD - Passwords 16. STANDARD - Privileged Account Creation & Management 17. STANDARD - User Account Creation & Management 18. STANDARD - Remote Access 19. STANDARD - Risk Management a. IT Risk Assessment Register b. PROTOCOL - Risk Management 20. STANDARD - Security Awareness & Training 21. STANDARD - Security Incident Response a. PROTOCOL - Security Incident Response b. PROTOCOL - Security Reporting c. PROTOCOL - Third Party Disclosure Approval 22. STANDARD - Zones Architecture 23. STANDARD - Wireless 24. STANDARD - Guest Wireless 25. STANDARD - Network Security 26. STANDARD - Physical IT Security a. PROTOCOL - Exception Request
Review Period:	3 years

Revision History:	New: October 1997 Revised: June 2013 Revised: May 2020 Revised: November 2023