DIGITAL SECURITY PROCEDURE

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

Category:	Information and Technology Management
Parent Policy:	E02 - Digital Security Policy
Approval Date:	April 14, 2020
Effective Date:	April 14, 2020
Procedure Owner:	CFO & Director / Director of 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 IT Security Procedure, in concert with the Digital Security Policy, describes the mechanism by which the Digital Security 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 IT 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.
Procedures:	The following are the Digital Security components that support the confidentiality, integrity and availability of Olds College digital data. These statements align with broadly accepted security practice and Digital Security Governance models relating to the following Digital Security categories: Governance & Compliance Policy, Standards, Guidelines & Procedures Security Architecture Risk & Change Management New Projects Participation Monitor, Assess & Reporting Security Incident Response, Investigations & Forensics Security Education & Awareness **Governance & Compliance** 1. The Director of IT, through the Chief Information Security Officer (CISO) and in consultation with the IT Security Advisory Working Group, shall oversee the Digital Security program and ensure that it is adequately enforced, regularly maintained and monitored for compliance and efficacy.

2. All information, such as contact lists, files, folders, email attachments and emails, sent or received on Olds College email systems are proprietary to Olds College and therefore considered to be institution property for records retention, legal and digital security purposes.
3. For the purposes of securing Olds College data in its various states, a Security Data Classification mechanism will be implemented that categorizes Olds College data into groups of like sensitivity.

Policy, Standards, Guidelines & Procedures

4. IT Security Standards, Procedures and any other relevant security instruments will be developed to support the overall intent of Digital Security Policy.

Security Architecture

5. Cryptographic technologies employed by Olds 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.
6. Olds College digital data will be disposed of in a manner that is appropriate for its level of sensitivity.
7. Internet facing applications will be protected utilizing a layered approach to security treatments.
8. Secure coding practices will be established and enforced for all application development.
9. 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.
10. Automated malware detection, prevention and correction mechanisms will be operated, monitored and maintained on all appropriate institution endpoints with access to digital information.
11. 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.
12. User Accounts/ID's granted access to resources on the Olds network will be unique, authorized, authenticated and managed through the creation of IT Security Standards and Procedures governing the authorization, creation, amending, suspending, removal and review of accounts/access privileges.
13. File shares/folder access will be carefully controlled and monitored ensuring that only authorized personnel may have access to stored information.
14. Passwords will be of appropriate length and complexity.
15. Remote access to Olds College Information Technology resources shall be permitted only through IT approved remote access methods.
16. 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.

Risk & Change Management

17. A Quantitative Risk Assessment Methodology will guide the application of IT Security controls throughout the Olds College environment.
18. 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.
19. The CISO, or designate, will be an integral member of the Change Advisory Board, to help ensure that IT changes to the Olds environment do not introduce unacceptable levels of risk.

New Projects Participation

20. The CISO, or designate, 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 Olds Digital Security Standards are met.

Monitor, Assess & Reporting

21. All devices that are or have connected to the Olds College network are subject to monitoring and/or auditing.
22. 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.
23. Metrics, suitable to demonstrate the efficacy of the overall Digital Security Program will be developed, maintained and reported to senior management.

Security Incident Response, Investigations & Forensics

24. 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.

Security Training & Awareness

25. A regular mandatory Digital Security training program will be administered and tracked which includes anyone with access to Olds College digital information.
26. The provision of occasional Digital Security Awareness for Olds College Staff/Faculty will be developed and offered to increase digital security awareness of the institution.
27. The process to enable these Policies is presented in the IT Security Procedure which outlines the identified approach.

	The IT Security Procedure will go through the standard process for approval by Olds college and once approved it establishes executive support for the creation of the IT Security Standards, Procedures and other instruments required to build a comprehensive security program. The formation of an IT Security Advisory Working Group, to provide general feedback on the broader IT Security Standards and other relevant instruments, will be undertaken. The IT Security Advisory Working Group will be governed by a charter that provides its mandate, operations and structure and may include ad-hoc representation from IT, Staff, Faculty, HR, Legal, Compliance and/or Risk. Once the IT Security Standards and other relevant instruments have been approved, a gap analysis will be undertaken to identify current disparities from the new IT Security Standards which may spawn a series of Digital Security projects, technology enhancements or procedural additions or adjustments. These projects, once completed, will position Olds College to be in alignment with the developed IT Security instruments. This process will be spread over several years. Once compliance has been achieved, a process will be established to verify that the IT Standards continue to be adhered to. In cases where there is incongruence, the issue(s) will be rectified as soon as possible. The Director of IT, through the Chief Information Security Officer (CISO) will be responsible to validate alignment with the approved Standards.
Exceptions:	A request for exception to this policy must be submitted for approval to the IT Director, which 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 Procedure. 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 Standard -** A specific Standard, explicit to a technology, usually a software or hardware build or deployment (for example, the following services will be disabled on a Windows 2019 Server…etc.) which dictates security configuration settings.
Related Information:	

Review Period:	3 Years Next Revision Date: May 2023
Revision History:	June 2013: New Policy May 2020: Major Revision