DIGITAL SECURITY POLICY

This document is the parent policy for any college or divisional procedures. Questions regarding this policy are to be directed to the identified Policy Administrator.

Functional Category:	Technology & Information
Approval Date:	June 14, 2017
Effective Date:	July 1, 2017
Policy Owner:	Vice President, College Services and Chief Financial Officer
Policy Administrator:	Director, Educational and Information Technologies

Objective:

NorQuest College (college) provides information assets such as computer devices, networks and electronic information systems to meet its mission, goals and initiatives. Access to these assets is a privilege. The purpose of this policy is to maintain the integrity and availability of college assets and to protect the confidentiality of associated data.

Authority to establish this policy is derived from the NorQuest College Board of Governors Policy No. 5 which delegates authority to the President and CEO to establish policies and procedures for the college's management and operation.

Policy:

The following are the Information Security Policy statements in support of confidentiality, integrity and availability of college digital data.

1. The Director of Education & Information Technology (E&IT), or designate, will ensure that Digital Security Standards, Procedures and any other relevant security instruments are developed to support the statements in this policy and good security practices; that they are adequately enforced, regularly maintained and monitored for compliance and efficacy ongoing.
2. All information, such as contact lists, files, folders, email attachments and emails, sent or received on the college email systems is proprietary to the college and therefore considered to be college property for records retention, legal and data security purposes.
3. Restricted and Confidential Data Classifications will not be disclosed to unauthorized third parties; will be transacted within a secure environment with security measures appropriate for the sensitivity of the data; and will be secured in such a way as to ensure that only intended recipients are able to access it.
4. 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.
5. College data will be disposed of in a manner that is appropriate for its level of sensitivity.
6. Internet facing applications will be protected utilizing a layered approach to security treatments.
7. Secure coding practices will be established and enforced for all application development.
8. Suitable standards, procedures, digital security baselines, and technological controls will be in place to ensure both the security of the network environment and protection of the security technologies in place.

9. Automated malware detection, prevention and correction mechanisms will be operated, monitored and maintained on all appropriate college endpoints with access to digital information.
10. 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.
11. User Accounts/ID's granted access to resources on the college network will be unique, authorized, authenticated and managed through the creation of standards and procedures governing the authorization, creation, amending, suspending, removal and review of accounts/access privileges.
12. File shares/folder access will be carefully controlled and monitored ensuring that only authorized personnel may have access to stored information.
13. Passwords will be of appropriate complexity.
14. Remote access to the college IT resources will be permitted only through E&IT approved remote access methods.
15. There will be no expectation of privacy on college computing resources. All devices that are or have connected to the college network are subject to monitoring and/or auditing.
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.
17. A Security Incident Response Team (SIRT) will be established and will be responsible for the creation and enablement of a SIRT Process to analyze, contain, eradicate, recover and learn from digital security events.
18. A Quantitative Risk Assessment Methodology will guide the application of IT Security controls throughout the college environment.
19. Regular Digital Security testing and/or risk assessments are performed to ensure compliance with established standards and digital security baselines to minimize risk due to changes within the environment, advancements in detection capabilities or newly identified threats to the organization.
20. IT Risks identified will be tracked, quantitatively rated and items identified to be above the organizations Risk Appetite will be targeted for remediation to lower the risk to an acceptable level.
21. The Director of E&IT, or designate, will be an integral member of the Change Advisory Board, to ensure that approved changes to the college environment do not introduce unacceptable levels of risk, and contribute on all new IT projects to allow for security measures to be designed into new solutions from inception.
22. A Regular Information Security awareness & training program will be administered and tracked.
23. Metrics, suitable to demonstrate the efficacy of the overall Security Program will be developed, maintained and reported to senior management.

Non Compliance

Any violation of this policy by an employee, temporary worker, contractor or vendor may result in, but not be limited to, disciplinary action and/or termination of their contract or assignment with the college. Any violation of this policy by a member of the Board of Governors may result in a recommendation to the Minister of Advanced Education to terminate their contract. As obligated by provincial and federal laws, the college will notify

	appropriate law enforcement agencies when any user has broken any laws or is known to have visited child pornography or hate crime web sites. **Exceptions** A request for exception to this policy is to be submitted to the Director of Education & Information Technology for approval as per the process described in the Information Security Exception Request Procedure. Exceptions may be granted for up to one year and will be reviewed regularly at which time the exception may be revoked, revalidated or extended for up to another one-year term. The list of exceptions will be maintained by E&IT.
Definitions:	**Digital Security Baseline:** 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 2012 server: [list of services]).
Related Information:	• Code of Conduct Policy
Related Procedures:	• Acceptable Use Standard (internal to college) • Digital Security Standards and Procedures
Next Review Date:	June 2021
Revision History:	June 2017: New. This policy and Digital Security Standards replace Computer and Internet Acceptable Use Policy, Printing Device Management Policy, Printing Device Selection and Allocation Procedure, Generic Network Account Policy and Procedure, Non-Student Username Change Policy and Procedure, Mobile Telephony Management Policy and Procedure, Remote Access Policy, Wireless Access Policy and Procedure, and Information Technology Process Change Control Policy.