



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 and Information
Approval date	May 13, 2025
Effective date	May 13, 2025
Policy owner	Vice President, Administration and Chief Financial Officer
Policy administrator	Director, Business Technology Services

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, Business Technology Services (BTS), 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 ongoing compliance and efficacy.

2. All information, such as contact lists, files, folders, email attachments, and emails sent or received on 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 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 and according to any provincial and/or federal requirements where applicable.
6. Internet-facing applications will be protected using a layered approach to security measures.
7. Secure coding practices will be established and enforced for all application development.
8. Suitable standards, procedures, 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. A cryptographic mechanism will be deployed and centrally managed when the sensitivity of the data involved or the mobility of the device warrants it.
11. User Accounts/IDs granted access to resources on the College network will be unique, authorized, authenticated, and managed according to established standards and procedures governing the authorization,

- creation, modification, suspension, removal, and review of accounts/access privileges.
12. 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 length and complexity.
 14. Remote access to College IT resources will be permitted only through BTS-approved remote access methods.
 15. All devices that are currently connected to the College network, or have previously connected, are subject to monitoring and/or auditing.
 16. Physical access to core IT devices will be secured so that only individuals who require access as part of their normal job functions are granted access.
 17. A Security Incident Response Team (SIRT) will be established and will be responsible for the creation and enablement of an Incident Response Process to identify, protect, detect, respond, 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 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 and quantitatively rated; items identified to be above the organization's Risk Appetite will be targeted for remediation to lower the risk to an acceptable level.
 21. The Director, BTS, or designate, will be a key member of the Change Advisory Board (CAB). Their role is to ensure that approved changes to the College environment do not introduce unacceptable levels of risk. Additionally, they will contribute to all new IT projects to ensure that security measures are integrated into new solutions from inception.
 22. A regular information security awareness and 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.

24. The use of cloud vendors will be assessed based on the classification of the data that is being used. Product vendors are required to provide appropriate assurance of their security measures.
25. In order to identify appropriate security treatments, a security data classification mechanism will apply to all College digital data.
26. Third-party service providers handling College data must adhere to the applicable College policies and standards and may undergo periodic security reviews.
27. All College IT assets must be inventoried, categorized, regularly scanned for vulnerabilities, and critical security patches must be applied based on a risk-based prioritization model.
28. The management of all College IT research assets, including the granting of access to third parties, will comply with the federal Policy on Sensitive Technology Research and Affiliations of Concern.

Non-Compliance

Any violation of this policy and any associated policies, procedures, standards, or guidelines 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 appointment. As obligated by provincial and federal laws, the College will notify appropriate law enforcement agencies when any user has broken any laws.

Exceptions

A request for exception to this policy is to be submitted to the Director, Business Technology Services (BTS), for approval as per the process described in the Exception Request Form. Exceptions may be granted for up to one (1) 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 BTS.

Definitions

Baseline: a specific standard, explicit to a technology, such as a software or hardware configuration or deployment. (For example, the following services will be disabled on a Windows 2022 server: [list of services]).

Related information

Link Accessibility

Some of the links included in this document are intended for internal use only. Please be aware that access to these links may be restricted to authorized personnel.

NorQuest College

- [Code of Conduct Policy](#)
- [Digital Security Standards](#)
- [Equity, Diversity and Inclusion](#)
- [Form - Exception Request](#)
- [Generative Artificial Intelligence Policy](#)

External

- [Policy on Sensitive Technology Research & Affiliations of Concern](#)

Next review date

June 2029

Revision history

Date	Version Number	Action
June 2017	V1	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.
August 2019	V2 (published as V1-C)	Compliance Office template and reorganization update
May 2021	V3 (published as V2)	Regular update interval with minor adjustments and added clause 24
February 2024	V4	Information, Risk & Compliance update
May 2025	V5	Digital Security engaged with Information, Risk & Compliance, the Faculty of Research & Academic Innovation, and the Cybera Shared Chief Information Security Officer to revise and enhance this version of the policy. The Policy has been updated to enhance clarity and alignment with the current organizational structure, while incorporating new elements related to compliance, security, and IT asset management. Additional updates were made to strengthen accountability and support related documentation.