



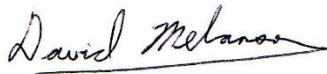
| | |
|-------------------|-------------------------------------------------------------------------|
| STANDARD | Glossary of Digital Security Standards, Policies, and Procedures |
| Owner: BTS | Approved Date: October 30, 2024 |

SUMMARY

The purpose of this standard is to support the secure use of NorQuest computer equipment. These rules are in place to protect both the employee and NorQuest. Inappropriate use of computer equipment exposes NorQuest to risks including virus attacks, compromise of network systems and services, availability of services and bandwidth in the pursuit of the organizational goals and legal issues. This standard enforces the principle of defense in depth and monitoring the effectiveness of security controls, while ensuring compliance with organizational, legal and regulatory requirements.

Business Technology Services (BTS) has the responsibility to ensure appropriate practices are adopted to conform to this standard and the Digital Security Policy that it supports.

APPROVAL

| | | | |
|---------------------|-----------------------------------------------------------------------------------|-----------------|-------------------------|
| Approved by: | David Melanson | Position | Director, BTS |
| Signature: |  | Date: | October 30, 2024 |

SCOPE

All digital systems utilized for the purpose of carrying out the mission of NorQuest College.

AUTHORITY

This standard has been created under the authority of Corporate Services & Finance and BTS which maintains the right to ensure that this standard is adhered to.

ENFORCEMENT

Any NorQuest employee found to have violated this standard may be subject to disciplinary action including, but not limited to, termination of employment. Any violation of the standard by a temporary worker, contractor or vendor may result in, but not limited to, the termination of their contract or assignment with NorQuest. As obligated by provincial and federal laws, NorQuest will notify appropriate law enforcement agencies when it appears that any applicable laws have been violated.

LINK ACCESSIBILITY

Note: 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.

EXCEPTIONS

A request for exception to this standard must be submitted for approval to the Director of BTS by following the process as described in the [Digital Security Exception Request Procedure](#). Granted exceptions will be for up to a one-year term and will be reviewed annually at which time the exception may be revoked, revalidated or extended for another one-year term. Exceptions will be maintained by BTS.



| | |
|-------------------|-------------------------------------------------------------------------|
| STANDARD | Glossary of Digital Security Standards, Policies, and Procedures |
| Owner: BTS | Approved Date: October 30, 2024 |

GLOSSARY OF TERMS

| Term | Definition | Source |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Authentication Protocol | A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of one or more valid authenticators to establish their identity, and, optionally, demonstrates that the claimant is communicating with the intended verifier. (A series of messages between a person trying to prove their identity and the verifier. It shows that the person has the right credentials and confirms they are talking to the correct verifier.) | NIST SP 800-63-3 |
| Availability | Ensuring timely and reliable access to and use of information. | NIST SP 800-137 |
| Certificate Authority (CA) | A trusted entity that issues and revokes public key certificates. | NIST SP 1800-16B |
| Certificate Revocation List (CRL) | A list of revoked public key certificates created and digitally signed by a certification authority. | NIST SP 800-12B |
| Confidentiality | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information | NIST SP 800-34 |
| Cybersecurity Event | Any observable occurrence in a network or system. This can include anomalies, warnings, or alerts. | NIST SP 800-61 |
| Demilitarized Zone (DMZ) | A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted. | NIST SP 800-16B |
| Intrusion Detection Systems (IDS) | Software that looks for suspicious activity and alerts administrators. | NISTIR 7711 |
| Incident | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information asset. | NIST SP 800-61 |
| Incident Response | The process of managing the aftermath of a security breach or cyberattack, including preparation, detection, and recovery. | NIST SP 800-61 |
| Incident Response Plan | The documentation of a predetermined set of instructions or procedures to detect, respond to, | NIST SP 800-34 |



| | |
|-------------------|-------------------------------------------------------------------------|
| STANDARD | Glossary of Digital Security Standards, Policies, and Procedures |
| Owner: BTS | Approved Date: October 30, 2024 |

| | | |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| | and limit consequences of a malicious cyber-attack against an organization’s information systems(s). | |
| Integrity | Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. | NIST SP 800-137 |
| Intermediate CA | A CA that is signed by a superior CA (e.g., a Root CA or another Intermediate CA) and signs CAs (e.g., another Intermediate or Subordinate CA). | CNSSI 4009-2015 from CNSSI 1300 |
| Intrusion Prevention Systems (IPS) | System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. | NISTIR 7711 |
| Likelihood | A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. | NIST SP 800-161r1 |
| Malware | Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. | NIST SP 800-137 |
| Multi-Factor Authentication (MFA) | An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are. | NIST SP 1800-17b |
| Network Inspection | Software that performs packet sniffing and network traffic analysis to identify suspicious activity and record relevant information. | NIST SP 800-86 |
| Patch Management | The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. | NIST SP 800-137 |
| Privacy | Assurance that the confidentiality of, and access to, certain information about an entity is protected | NIST SP 800-10B |
| Recovery Time Objective (RTO) | The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes. | NIST SP 800-34 |
| Risk | A measure of the extent to which an entity is threatened by a potential circumstance or event | NIST SP 800-30 |



| | |
|-------------------|-------------------------------------------------------------------------|
| STANDARD | Glossary of Digital Security Standards, Policies, and Procedures |
| Owner: BTS | Approved Date: October 30, 2024 |

| | | |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Risk Management | The program and supporting processes to manage information security risk to organizational operations. | NIST SP 800-39 |
| Root CA | In a hierarchical Public Key Infrastructure (PKI), the Certification Authority (CA) whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. | NIST SP 1800-21C |
| Secure Channel | A path for transferring data between two entities or components that ensures confidentiality, integrity and replay protection, as well as mutual authentication between the entities or components. | NIST SP 800-90A |
| Spoofing | Faking the sending address of a transmission to gain illegal entry into a secure system. | NIST IR 8323r1 |
| Threat | Any circumstance or event with the potential to cause harm to an information system or organization. | NIST SP 800-61 |
| Virus | A computer program that can copy itself and infect a computer without permission or knowledge of the user. | NIST SP 800-12 |
| Vulnerability | A weakness in a system, application, or process that could be exploited by a threat actor. | NIST SP 800-61 |

REVISION AND REVIEW HISTORY

This Standard is to be reviewed annually, with the allowance for ad hoc changes as required.

| Date | Version | Evaluation | Author | Summary |
|---------------|---------|---------------|-------------------------|--------------------------------------|
| Oct 7, 2024 | 0.1 | Initial Draft | Gurdev Singh | Creation of the document. |
| Oct 18, 2024 | 0.2 | Revision | Gero Schaefer | Incorporating the feedback received. |
| Oct 24, 2024 | 0.3 | Revision | Daniel Queiroz del Lama | Added Spoofing. |
| Oct 28, 2024 | 0.4 | Revision | Gero Schaefer | Added Link Accessibility section. |
| Oct. 30, 2024 | 0.5 | Revision | Dave Melanson | Corrected minor grammatical errors. |
| Oct 30, 2024 | 1.0 | Review | Dave Melanson | Approved Version |