Policy Title: Information Security Policy

Policy Number: ITO.102

Policy Owner: Director of Business Affairs

Responsible Office: Information Technology (IT) Office

Revision Date: 6/15/2016

---

1. Purpose and Scope

North American University (NAU) Information Security Policy describes the role of information security in supporting the academic, research and business mission of NAU through the recognition of the growing importance of securing electronic resources. This document identifies key security issues for which individuals, departments, and units are responsible.

This policy applies to all NAU locations and all system users at any location, including those faculty, students and staff using privately owned computers or systems to access NAU information, computing and network resources.

2. Policy

Every member of the university community is responsible for protecting the security of university information and information systems by adhering to the objectives and requirements stated within published university policies. Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action.

Violations of this and related policies will be handled according to NAU disciplinary procedures based on the person or persons responsible for the violation. Violations of local, state, federal or other laws will be reported to the appropriate, respective authorities.

3. Definitions

Chief Technology Officer (CTO)

Chief Technology Officer has overall responsibility for the security of the NAU's information technologies. Responsibilities include:

- Develop university-wide information security policies, procedures, and guidelines.
- Implement a university-wide security program, including policy, procedure and best practice development, user education and training and ongoing network and security risk analysis.
- Lead investigations and reporting of information security incidents, acting as the point of contact when working within NAU departments and outside parties.

User

A user is anyone who uses an IT Resource. User responsibilities are as follows:

- Users are expected to be familiar with and follow NAU policies, guidelines and procedures related to information and network security.
- Users are responsible for the protection of confidential, sensitive and other university-related information entrusted to them.

Users who use personally-owned systems to access NAU resources are responsible for the security of their

personally-owned computers or other network devices and are subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by IT Office for university computing and network facilities.
- All other laws, regulations, or policies directed at the individual user

4. Procedures

Security requirements shall be in place for the protection of the privacy of information, protection against unauthorized modification of information, protection of systems against the denial of service, and protection of systems against unauthorized access.

The following system requirements represent the minimum standard that must be in place in order to establish and maintain security for NAU information, computing and network resources.

Password Specification

All passwords on any system, whether owned by NAU or by an individual, directly connected to NAU network must adhere to the following standards when technically possible. This includes devices connected to the campus network with a direct wired connection, wireless, remote access software (e.g., Windows Remote Desktop), use of a Virtual Private Network (VPN), and the like. Any system that does not comply may have its network access blocked without prior notification.

Passwords must:

- have a minimum of 7 characters.
- not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (for example, !, $, #, %)

The following complexity requirements are enforced when passwords are changed or created.

- Passwords must be changed at least twice a year (maximum password age is 200 days, minimum password age is 1 day).
- Passwords must be changed significantly and cannot repeat more frequently than every two years (Past 5 passwords are kept in the system).

Users using any NAU system password shall abide the following rules:

- Passwords that are written down or stored electronically must not be accessible to anyone other than the owner and/or issuing authority.
- Passwords must not be shared unless explicitly permitted by the issuing authority.
- Anyone who believes their password has been compromised must immediately notify the IT Office to evaluate possible risks.
- Default passwords in vendor-supplied hardware or software must be changed during initial installation or setup.

Unattended Computers

To protect against unauthorized access to data on computers left unattended, the following precautions are required:

- Enable password protection on the screen saver for all university computers with the exception of special-purpose computers designed for public access, such as information or registration kiosks, , or computer labs where locking is undesirable due to the risk of a user monopolizing a shared computer. The length of time before the password-protected screen saver comes on should be set to 20 minutes or less.
- For computer labs, it is recommended that computers be set to automatically logout after 30

minutes of idle time.

- Never leave your computer unattended and unprotected. Before leaving your computer, lock the display or log out in a manner that requires a password to gain access.

Protection from Malicious Software and Intrusions

Malicious software, or "malware", comes in many forms - viruses, worms, Trojan horses, denial of service attacks, botnets, spyware, adware, spam relays, etc. All pose a security risk, some of which are a very serious threat to the confidentiality, integrity, or availability of NAU's information and technology resources. To that end, NAU may require the installation of essential security software on computers connected to the NAU campus network or accessing NAU information and technology resources.

Reporting of Security Incidents

A critical component of security is to address security breaches promptly and with the appropriate level of action. All individuals are responsible for reporting incidents IT Office in which they suspect data, computer or network security may have been compromised.

Violations

Violations as related to this policy are generally considered:

- Any action of malicious intent (breaking into a system, purposefully sending a virus or other piece of malicious software to other computers, etc.);
- Any action designed to circumvent applied computer security (accessing data for which the User does not have authorized access, disabling system and security logging, etc.);
- Any action that scans, sniffs or logs systems or networks without authorization from the IT Office.

Also, systems that appear to be infected or compromised may be disconnected from the network until the system is remedied. The IT Support Team will attempt to notify the owner for the system when it is taken offline.

Enforcement

Any device directly connected to the campus network (i.e., with a direct wired or wireless connection, dial-in modem, remote access software like Windows Remote Desktop, use of a Virtual Private Network (VPN), and the like) may be scanned and assessed by IT Support Team at any time to determine compliance with security policies and standards, or detect anomalous activities, vulnerabilities, and security compromises. Firewalls must be configured to permit this remote scanning function. Scanning may only be performed to the extent necessary to detect and assess the risk.

5. Who Should Read This Policy

- Students
- Faculty and Staff