NORTH AMERICAN UNIVERSITY
INSPIRATION INNOVATION GLOBAL COMPETENCE
HOUSTON, TEXAS
WWW.NA.EDU

APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY

Effective Date: 08/01/2014 1. **Policy**

North American University's (NAU) Appropriate Use of Information Technology Resources policy provides for access to information technology (IT) resources and communications. These resources are vital for the fulfillment of the academic, research and business needs of the University community within a culture of openness, trust, and integrity. In addition, NAU is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

2. **Reason for Policy* (Purpose)**

The purpose of this policy is to outline the ethical, acceptable and appropriate use of information systems and resources at NAU. These rules are in place to protect University community (e.g., all faculty, staff, students, and alumni) to ensure that they have access to reliable, robust IT resources that are safe from unauthorized or malicious use.

3. Scope

This policy applies to the entire University community (e.g., all faculty, staff, students, and alumni) as well as any other individuals or entities who use information and IT resources at NAU. This policy also applies to all IT resources owned or leased by NAU and to any privately owned equipment connected to the campus network and includes, but is not limited to, computer-related equipment, software, operating systems, storage media, the campus and interconnecting networks as well as all information contained therein.

4. **Appropriate Use**

Appropriate use of NAU Information Technology resources is consistent with the education, research, and service needs of the University. Appropriate use of Information Technology resources includes instruction; independent study; authorized research; independent research; and official duties of the offices, units, recognized student and campus organizations, and agencies of the NAU.

Authorized users are provided access in order to support their studies, instruction, duties as employees, official business with the university, and other university-sanctioned activities. Authorized users are: (1) faculty, staff, and students of the NAU; (2) anyone connecting to NAU's IT resources with authorization; (3) others whose access furthers the mission of NAU and whose usage does not interfere with other users' access to resources.

It is authorized users' responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to continuously verify the integrity and completeness of information that users compile or use. Authorized users are responsible for the security and integrity of NAU information stored on the individual computing desktop system.

5. Inappropriate Use

5.1. Excessive Non-Priority Use of Computing Resources

Priority for the use of IT resources is given to activities related to the NAU's missions of teaching, learning, research, and outreach. NAU computer and network resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of IT resources, such as recreational activities and non-academic, non-business services.

5.2. Unacceptable system and network activities include:

- Obtaining configuration information about a network or system for which the user does not have administrative responsibility.
- Engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network.
- Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.
- Interfering with or denying service to another user on the campus network or using university facilities or networks to interfere with or deny service to persons outside the university.
- Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program).

5.3. Unauthorized Use of Intellectual Property

Users may not use university facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

- Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.
- Using, displaying, or publishing licensed trademarks, including NAU’s trademarks, without license or authorization or using them in a manner inconsistent with the terms of authorization.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.
- Using computing facilities and networks to engage in academic dishonesty prohibited by university policy (such as unauthorized sharing of academic work or plagiarism).

5.4. Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

- Setting up file sharing in which protected intellectual property is illegally shared.
- Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Inappropriate use or sharing of university-authorized IT privileges or resources.
- Changing another user's password, access, or authorizations.
- Using an NAU computing asset to actively engage in displaying, procuring, or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.
- Using an NAU computing asset for any private purpose or for personal gain.
- Using NAU resources for one's own commercial gain, or for other commercial purposes not officially approved by the NAU, including web ads.
- Using NAU resources to operate or support a non-University related business.

- Use of NAU resources in a manner inconsistent with the NAU's contractual obligations to suppliers of those resources or with any published NAU policies.

5.5. Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of NAU and to individual communication among faculty, staff, students, and their correspondents. Individuals are required to know and comply with the NAU's policy on Email Communication. Key prohibitions include:

- Sending unsolicited messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material, except as approved under the policy on Email Communication.
- Engaging in harassment via electronic communications whether through language, frequency, or size of messages.
- Masquerading as someone else by using their email or internet address or electronic signature.
- Soliciting email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or solicitations for business schemes.
- Using email originating from NAU provided accounts for commercial use or personal gain.
- Transmitting unsolicited information that contains obscene, indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct.
- Using e-mail or newsgroups to threaten or stalk someone.
- Transmitting unsolicited information that contains profane language or panders to bigotry, sexism, or other forms of prohibited discrimination.
- Broadcasting e-mail from a university account to solicit support for a candidate or ballot measure, or otherwise using e-mail systems in a concerted effort to support a candidate or ballot measure.

5.6. Damage or impairment of NAU resources:

- Use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently (1) damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program), (2) damaging or violating the privacy of information not belonging to you, or (3) misusing or allowing misuse of system resources.
- Use of NAU resources for non-University related activities that unduly increase network load (e.g., chain mail, network games and spamming).

5.7. Interference or impairment to the activities of others:

- Creating, modifying, executing or retransmitting any computer program or instructions intended to: (1) obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic e-mail; (2) bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner; or (3) examine or collect data from the network (e.g., a "network sniffer" program).
- Authorizing another person or organization to use your computer accounts or NAU network resources. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not share your password with anyone else or provide access to NAU network resources to unauthorized persons.
- Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.

5.8. Violation of city, state or federal laws:

- Pirating software, music and images.
- Effecting or receiving unauthorized electronic transfer of funds.
- Disseminating child pornography or other obscene material.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

6. **Enforcement**

Reports of unauthorized use or misuse of the resources will be investigated pursuant to standard University procedures. All illegal activities will be reported to local, state or federal authorities, as appropriate, for investigation and prosecution. NAU reserves the right to investigate unauthorized or improper use of NAU resources, which may include the inspection of data stored or transmitted on the network. In the event that use is determined to be contrary to NAU policy or applicable law, appropriate measures will be taken. These measures may include, but are not limited to, permanent or temporary suspension of user privileges, deletion of files, and disconnection from the NAU network, referral to student or employee disciplinary processes, and cooperating with the appropriate law enforcement officials and government agencies.

The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms.

Interim Measures

NAU may temporarily disable service to an individual or a computing device, when an apparent misuse of university computing facilities or networks has occurred, and the misuse:

- Is a claim under the Digital Millennium Copyright Act (DMCA)
- Is a violation of criminal law
- Has the potential to cause significant damage to or interference with university facilities or services
- May cause significant damage to another person
- May result in liability to the university

An attempt will be made to contact the person responsible for the account or equipment prior to disabling service unless law enforcement authorities forbid it or Information Technology Services staff determine that immediate action is necessary to preserve the integrity of the NAU network. In any case, the user shall be informed as soon as possible so that they may present reasons in writing why their use is not a violation or that they have authorization for the use.

Suspension of Services

Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if:

- After hearing the user's explanation of the alleged violation, an IT Department has made a determination that the user has engaged in a violation of this code, or
- A student or employee disciplinary body has determined that the user has engaged in a violation of the code.

7. **Contacts**

The examples of unauthorized use set forth above are not meant to be exhaustive. Questions about this policy or of the applicability of this policy to a particular situation should be referred to at cto@na.edu. Chief Technology Officer is the final authority on questions of appropriate use of University resources.

NORTH AMERICAN UNIVERSITY
INSPIRATION INNOVATION GLOBAL COMPETENCE
HOUSTON, TEXAS
WWW.NA.EDU

EMAIL COMMUNICATION POLICY

Effective Date: 08/01/2014

1. Policy

This policy outlines rules and standards to electronic mail. E-mail is considered a formal communication by North American University (NAU). Users are reminded that all usage of NAU's information technology resources including electronic mail is subject to all University policies including the Appropriate Use of Information Technology Resources.

2. Policy Statement (Reasons)

NAU must be able to communicate quickly and efficiently with faculty, staff, and students in order to conduct university business. Email is an acceptable and appropriate medium for such communications. NAU may send communications to faculty, staff, and students by email to their NAU email address. Faculty, staff and students are expected to check their e-mail on a frequent and consistent basis in order to stay current with University and/or faculty-student related communications. This includes communications intended to meet the academic and administrative needs of the university, including business that is critical to the operation and function of NAU.

3. Security & Privacy

Electronic mail and data stored on the NAU's network of computers and email servers may be accessed by NAU IT Support Team for the following purposes:

- troubleshooting hardware and software problems,
- preventing unauthorized access and system misuse,
- retrieving University business related information, *
- investigating reports of alleged violation of University policy or local, state or federal law,*
- complying with legal requests (e.g.; court orders) for information, * □ rerouting or disposing of undeliverable mail, □ addressing safety or security issues.

* The system administrator will need written approval, including e-mail, indicating the extent of access that has been authorized from the Vice President for Administrative Affairs, to access specific mail and data for these purposes.

Email communications must comply with federal and/or state regulations and university policies including the Appropriate Use of Information Technology Resources. NAU will not request personal confidential information such as social security, credit/debit card, or bank account numbers be returned by email. Faculty, staff, and students are responsible for keeping their email passwords confidential, and must not share their password with others or leave it exposed. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved.

4. University Email Address

University email addresses are of the form *userid*@na.edu (previously userid@northamerican.edu) and are included in university directory information. Current NAU students are expected to have a University user ID and email address.

The University user ID and email address will be suspended after the effective date of termination or separation from the university. An email address of the users may be restored and maintained by a university administrative officer for the purpose of carrying out university business.

5. Forwarding

Although students or employees may choose to forward their university email address to another email address, there is a risk forwarded email may be lost or blocked. Problems with forwarded email will not absolve the individual of responsibilities associated with university communications sent to their university email address.

6. Instructional Use

Faculty will determine how electronic communication, including email, will be used in their classes, and must specify those requirements in the course syllabus.

7. Violation

Violations of University policies governing the use of this policy may result in restriction of access to University information technology resources in addition to any disciplinary action that may be applicable under other University policies, guidelines or implementing procedures, up to and including dismissal.

8. Policy Scope

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.

9. Contacts

Questions about this policy or of the applicability of this policy to a particular situation should be referred to at cto@na.edu. Chief Technology Officer is the final authority on questions of appropriate use of email communications.

NORTH AMERICAN UNIVERSITY
INSPIRATION INNOVATION GLOBAL COMPETENCE
HOUSTON, TEXAS
WWW.NA.EDU

INFORMATION SECURITY POLICY

Effective Date: 08/01/2014

1. Policy

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. NAU acknowledges its obligation to ensure appropriate security for IT (Information Technology) systems in its domain of ownership and control.

2. Policy Statement (Reasons)

Protecting and preserving IT resources and complying with applicable laws and regulations are common, shared responsibilities for all members of the NAU community. Every member of the NAU community is responsible for protecting the security of NAU information and information systems by adhering to the objectives and requirements stated within this policy.

3. Roles and Responsibilities

3.1 Chief Technology Officer (CTO)

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

- Develop university-wide information security policies, procedures, and guidelines through working with representative groups on campus.
- 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 with other NAU groups.

3.2 User

A user is anyone who uses an IT Resource. Users have a responsibilities as follows:

- All Users are expected to be familiar with and follow NAU policies, guidelines and procedures related to information and network security.
- Other groups on campus, many at the department level, may have group-specific policies and guidelines. If these exist, the Users in those groups are also expected to be familiar with and follow them as well.
- All Users are responsible for the protection of confidential, sensitive and other university-related information entrusted to them as well as prevent disclosing such data to unauthorized party.

3.3 Individuals Using Personally-Owned Computers and Other Network Devices

Students, faculty, and staff 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 Support Team for university computing and network facilities.
- All other laws, regulations, or policies directed at the individual user.

3.4 Other Registered Entities

Any entity that is a registered user and connected to the university network is responsible for the security of its computers and network devices and is subject to the following:

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

4. Requirements for Information, Computing and Network Security

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.

4.1 Password Specification:

Password Policy: 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.

Password Standards:

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-alphabetic characters (for example, !, $, #, %)

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).

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 Support Team to evaluate possible risks.

Default passwords in vendor-supplied hardware or software must be changed during initial installation or setup.

4.2 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, public computers in the library, 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 lab situations, it is recommended that computers be set to automatically logout after at the most 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.

4.3 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.

5. 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 in which they suspect data, computer or network security may have been compromised.

6. 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 Support Team;

Also, systems that appear to be infected or compromised to the IT Support Team 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.

7. 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.

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.

8. Policy Scope

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.

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.

9. Contacts

Questions about this policy or of the applicability of this policy to a particular situation should be referred to at cto@na.edu. Chief Technology Officer is the final authority on questions of appropriate use of email communications.