NORTH AMERICAN UNIVERSITY

INSPIRATION INNOVATION GLOBAL COMPETENCE

Policy Title: Appropriate Use of Information Technology Resources Policy

Policy Number: ITO.101

Policy Owner: Director of Business Affairs

Responsible Office: Information Technology (IT) Office

Revision Date: 6/15/2016

---

1. Purpose and Scope

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 the University community (e.g., all faculty, staff, students, and alumni), as well as to ensure that all members of that community have access to reliable and robust IT resources free from unauthorized or malicious use.

This policy applies to the entire University community (e.g., all faculty, staff, students, and alumni) as well as to any other individuals or entities who utilize 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, including but not limited to technological hardware, software, operating systems, storage media, the campus and its interconnecting networks and all information contained therein.

2. Policy

North American University provides a variety of information technology resources that are vital for the fulfillment of the academic, research and business needs of the University community within a culture of transparency, honesty, and integrity. Access to these resources is a privilege and governed by certain regulations and restrictions. Each person who accesses or uses university information technology resources accepts the responsibilities outlined here and in other university policies and standards. In addition, users will adhere to applicable local, state and federal laws and regulations.

3. Definitions

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, research, and official duties of the offices, units, recognized student and campus organizations, and agencies of the NAU.

Authorized users are provided access 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) guests/temporary users connecting to NAU's IT resources; and (3) others whose access furthers the mission of NAU and whose usage does not interfere with other users' access to resources.

It is the responsibility of an authorized user to be aware of the potential for and possible consequences of manipulating information, especially in electronic form, and 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 electronic devices.

Inappropriate Use

I. 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.

II. Unacceptable System and Network Activities

Unacceptable system and network activities include, but are not limited to the following:

- 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).

III. 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 the following:

- 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).

IV. Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes, but is not limited to the following:

- 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.

V. 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.

VI. Damage or Impairment of NAU Resources

Damage includes but is not limited to the following:

- 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).

VII. Interference or Impairment to the Activities of Others

Interference or impairment to technology activities includes, but is not limited to the following:

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.

VIII. Violation of City, State or Federal laws

Possible violations of the city, state, and federal laws include, but are not limited to the following:

- 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.

4. Procedures

Reports of unauthorized use or misuse of NAU IT 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 by NAU. These measures may include, but are not limited to: permanent or temporary suspension of user privilege; deletion of files; 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, IT Office 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.

5. Who Should Read This Policy

- Students
- Faculty and Staff

6. Related Documents and References

- Email Communication Policy