1.0 Overview

IT Security’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to NSU Florida’s (NSU) established culture of openness, trust and integrity.

IT Security is committed to protecting NSU’s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of NSU. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of everyone at NSU who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at NSU. These rules are in place to protect the employees, students, and NSU. Inappropriate use exposes NSU to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy provides guidelines for the appropriate and inappropriate use of the computing resources of NSU. It applies to all users of the University's computing resources including students, faculty, staff, alumni, and guests of the University. Computing resources include all computers, related equipment, software, data, and local area networks, both wired and wireless, for which the University is responsible.

The computing resources of NSU are intended to be used for its programs of instruction and research and to conduct the legitimate business of the University. All users must have proper authorization for the use of the University's computing resources. Users are responsible for seeing that these computing resources are used in an effective, ethical, and legal manner. Users must apply standards of normal academic and professional ethics and considerate conduct to their use of the University's computing resources. Users must be aware of the legal and moral responsibility for ethical conduct in the use of computing resources. Users have a responsibility not to abuse the network and resources, and to respect the privacy, copyrights, and intellectual property rights of others.
In addition to the policy contained herein, usage must be in accordance with applicable University Policies and applicable State and Federal laws. Among the more important laws are the Florida Computer Crimes Act, the Federal Computer Abuse Amendment Act 1994, the Federal Electronic Communications Privacy Act, and the U.S. Copyright Act.

4.0 Policy

4.1 General Use and Ownership

- While NSU’s IT administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of NSU. Because of the need to protect NSU’s network, management cannot guarantee the confidentiality of information stored on any network device belonging to NSU.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within NSU may monitor equipment, systems and network traffic at any time under the direction and prior approval of the CIO.
- NSU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords will be changed in accordance with the NSU Enterprise Username and Password Policy.
- All PCs, laptops and workstations should be secured with a screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
- Use encryption on devices and systems where feasible and as directed by OIIT.
- Postings by employees from NSU email addresses to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NSU, unless posting is in the course of business duties.
- All hosts used by the employee that are connected to the NSU Internet/Intranet/Extranet, whether owned by the employee or NSU, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of NSU authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NSU-owned resources.
The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NSU.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NSU or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using NSU computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any NSU account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior approval from the Chief Information Security Officer is granted.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, NSU employees to parties outside NSU.

4.3.2 Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
• Unauthorized use, or forging, of email header information.
• Solicitation of email for 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", "Ponzi" or other "pyramid" schemes of any type.
• Use of unsolicited email originating from within NSU’s networks to others.
• Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NSU or connected via NSU's network.

4.4. Blogging

• Blogging by employees, whether using NSU’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of NSU’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate NSU’s policy, is not detrimental to NSU’s best interests, and does not interfere with an employee's regular work duties. Blogging from NSU’s systems is also subject to monitoring.
• NSU’s Confidential Information policy also applies to blogging. As such, employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by NSU’s Confidential Information policy when engaged in blogging.
• Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of NSU and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by NSU’s Non-Discrimination and Anti-Harassment policy.
• Employees may also not attribute personal statements, opinions or beliefs to NSU when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of NSU. Employees assume any and all risk associated with blogging.
• Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, NSU’s trademarks, logos and any other NSU intellectual property may also not be used in connection with any blogging activity.

5.0 Enforcement

Inappropriate conduct and violations of this policy will be addressed by the appropriate procedures and agents (e.g., the Office of the Dean, the Office of the Vice President for Academic Affairs, or the Office of Human Resources) depending on the individual's affiliation to the University. In cases where a user violates any of the terms of this policy, the University may, in addition to other remedies, temporarily or permanently deny access to any and all NSU computing resources, and appropriate disciplinary actions may be taken, up to and including dismissal. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Timeline

Effective Date: Upon Implementation

Review Date: Annually