Acceptable Use Policy

1.0 Purpose

The inappropriate and/or improper use of Nova Southeastern University's ("NSU") computer systems and equipment can expose the University to a variety of risks, including, but not limited to, virus attacks, compromised network systems and services, and legal issues. As such, NSU, in coordination with IT Security, is committed to protecting the University and its faculty, employees, students, and partners from damaging actions arising from such inappropriate or improper use by setting forth this Policy to outline the acceptable use of NSU's computer systems and equipment.

Effectively securing NSU's computer systems is a team effort that involves the participation and support of every individual at NSU who deals with information and/or information systems. Therefore, it is the responsibility of every NSU computer user to read and familiarize themselves with this Policy and to conduct themselves accordingly.

2.0 Scope

This Policy provides guidelines pertaining to the appropriate and acceptable use of NSU's computing resources, including, but not limited to, internet, intranet and extranet-related systems, such as computers and related equipment, software, data, operating systems, storage media, WWW browsing, network accounts providing electronic mail, and local area networks for which the University is responsible. This scope of this Policy applies to all NSU computer users, including students, faculty, staff, alumni, and guests of the University.

In addition to the Policy contained herein, usage of NSU's computing resources must be in accordance with applicable University policies and State and Federal laws, including, but not limited to, the Florida Computer Crimes Act, the Federal Computer Abuse Amendment Act of 1994, the Federal Electronic Communications Privacy Act, and the U.S. Copyright Act.
3.0 **Policy**

3.1 **General Use and Ownership**

- All NSU computer users must obtain proper authorization to use and access the University's computing resources.
- NSU computer users are responsible for ensuring that they use the University's computing resources in an effective, ethical, and legal manner. Users must apply standards of normal academic and professional ethics and exercise considerate conduct when utilizing such computing resources.
- NSU computer users have a responsibility not to abuse the University's computing network and resources, and to respect the privacy, copyrights, and intellectual property rights of others.
- NSU's computing resources are the property of NSU and are therefore intended to be used in furtherance of its academic programs of instruction, for research purposes, and to conduct the legitimate business of the University.
- While NSU's IT administration desires to provide NSU computer users with a reasonable level of privacy, users should be aware that the data they create and/or store on the University's computing systems remains the property of NSU. Because of the need to protect NSU's computing resources, NSU cannot guarantee the confidentiality of information stored on any network device belonging to the University.
- NSU computer users are responsible for exercising sound judgment regarding the reasonableness and extent of personal use of University computing systems. However, while not prohibited, users should be aware that private and personal information placed on NSU computing resources may be subject to search and removal without prior notice. There should be no expectation of privacy when using a NSU computer system. Every component of data, in whatever form, contained on a NSU computer or storage system is the property of NSU and, as such, NSU has the right to use said data contained on the computer or storage system for whatever purpose it deems necessary in its sole discretion.
- Individual departments are responsible for creating guidelines pertaining to NSU computer users' personal use of Internet/Intranet/Extranet systems. In the absence of such policies, NSU computer users should consult their immediate supervisor or manager for guidance.
- For security and maintenance purposes, authorized individuals within NSU may monitor the University's equipment, systems, and network traffic at any time under the direction and prior approval of the NSU Chief Information Officer (“CIO”).
- NSU reserves the right to audit the University’s computing networks and systems on a periodic basis to ensure compliance with this Policy.
- As the information and data contained within NSU’s computing systems is the property of NSU, NSU Administration, under the direction of the NSU CIO, has the right to review such information and data to ensure and enforce compliance with this Policy.
3.2 Security and Proprietary Information

- Authorized NSU computer users are responsible for maintaining the security of their passwords and may not share accounts with any other individual. System- and user-level passwords shall be changed annually in accordance with the NSU Enterprise Username and Password Policy.
- All PCs, laptops and workstations should be secured with a screen saver with the automatic activation feature set at ten (10) minutes or less, or by logging-off when the host will be unattended, unless an appropriate exception has been granted, in writing, by the NSU Chief Information Security Officer.
- Use encryption on devices and systems where feasible and as directed by the NSU Office of Innovation and Information Technology (“OiiT”) and other applicable University policies.
- Any NSU computer user who connects a personal device to a NSU network shall ensure that such device has appropriate security controls, including anti-virus software, if possible.
- 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. Employees will be held accountable for any negligent handling of e-mail attachments that would appear, to a reasonable person, to potentially create any of the problems listed in Section 3.3, below.

3.3 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 Nova Southeastern University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing University-owned resources.

The lists of unacceptable uses of University computing resources, below, are by no means exhaustive, but are intended to provide a general framework of prohibited activities. If a NSU computer user has a question as to whether an activity that is not listed below is considered an acceptable use of NSU’s computing resources, NSU IT Security should be contacted prior to engaging in such activity.

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, pursuant to the NSU Organization Software Policy.

- Unauthorized copying, distribution, alteration and/or translation 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.
- 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, including family and other household members when work is being done at home, pursuant to the NSU Enterprise Username and Password Policy.
- Using NSU's computer systems to impersonate another individual, whether or not such individual is affiliated with NSU.
- Using a NSU computing asset 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 University 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 University duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffig, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning, unless prior approval from the NSU Chief Information Security Officer has been granted.
- Executing any form of network monitoring that 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).
- Engaging in any actions that disrupt or interfere with the legitimate use of NSU's computer systems by other NSU computer users, including, but not limited to, 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 of the University.
• Engaging in any other inappropriate uses of the computer that fall below the standard of care and the general standards of the industry.

**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.
• Possessing, distributing, or sending unlawful communications of any kind, including, but not limited to, threats of violence, obscenity, pornography, child pornography, and/or any form of harassment, as defined by law, or participating or facilitating communications in furtherance of any illegal activities.
• 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.

### 3.4. Blogging & Internet Postings

• Blogging by NSU employees on NSU’s computer systems is prohibited, unless such blogging is conducted for a legitimate business purpose of the University and the employee is permitted to do so pursuant to his or her NSU job description.
• NSU employees are prohibited from revealing any confidential, proprietary and/or sensitive information, as well as any trade secrets, of the University when engaged in blogging or any other form of Internet posting.
• Employees may also not attribute personal statements, opinions or beliefs to NSU when blogging.
• Employees assume any and all risks associated with blogging.
• Pursuant to NSU’s Social Media Policy, postings by employees using a NSU e-mail address to newsgroups or other Internet websites should contain a disclaimer stating that the opinions expressed by the individual are strictly their own and do not necessarily represent those of NSU, unless such posting is in the course and scope of the employee’s University business duties.
• Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, NSU’s trademarks, logos and any other University intellectual property may not be used in connection with any blogging activity.
4.0 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 NSU computer 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

Approvals

[Signatures]

President & Chief Executive Officer

Executive Vice President & Chief Operating Officer

[Dates]

3/30/15

3/30/15

APPROVED AS TO LEGAL FORM

Signature: [Signature]

Print Name: Thomas Panza

Panza, Maurer Maynard, P.A.

APPROVED AS TO BUSINESS CONTENT

Signature: [Signature]

Print Name: Tom West

Innovation & Information Technology

NSU ACCEPTABLE USE POLICY
PAGE 6 OF 6