| SUPERSEDES:NEW | CODE NO: SEC13 |
|---|---|
| NOVA SOUTHEASTERN UNIVERSITY | SECTION: IT SECURITY |
| | SUBJECT: *COMPUTER SECURITY DEVICE STANDARDS POLICY* |

**Purpose**

Nova Southeastern University's (NSU) network and information systems provide the technical foundation for conduct of its academic, research and administrative missions. Providing this open access to information technology is imperative to ensuring academic freedom at the institution. An important part of providing this access is ensuring that the devices and associated information is secure.

The purpose of this policy is to provide guidance to faculty, staff, students and other authorized users regarding device security policy and standards in regards to NSU owned devices including Windows based PC's, tablets, servers, as well as systems that run on other operating systems such as MAC, LINUX, UNIX, etc.

**Scope**

This policy applies to all employees and faculty of Nova Southeastern University (NSU); as well as vendors, contractors, partners, students, collaborators and any others doing business or research with NSU will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving NSU owned computers, technology systems, and/or data will also be subject to the provisions of this policy.

**Policy**

- **Device Management**

  All NSU owned devices will be managed by the Office of Innovation and Information Technology (OIIT) via device management software. This includes NSU owned servers, PC's, laptops, tablets, and smart phones (the "Devices").

- **Anti-Virus/Anti-Malware**

  All NSU owned devices will be covered by reasonable anti-virus and anti-malware software to manage the protection of the devices and information on NSU's network.

  The OIIT's responsibilities regarding anti-virus and anti-malware include, but are not limited to the following:

  - installing anti-virus/anti-malware software on all NSU owned Devices;

- keeping the anti-virus/anti-malware software up-to-date; and
- taking appropriate actions to contain virus infections and assist in the recovery from virus or malware infections on NSU owned Devices.

The Users of NSU owned Devices must adhere to the following guidelines to support the anti-virus/anti-malware protections of the University:

- Users must not attempt to alter or disable antivirus software on any NSU owned Device;
- Users must not open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source;
- Users should delete Spam, chain, and other junk email without forwarding it; and
- Users must not download files from unknown or suspicious sources.

When an NSU owned Device is determined to be infected with a virus or other malicious software, the following procedures shall be followed:

1) NSU OIIT will configure the anti-virus products to try to automatically remove any viruses or malware detected on NSU owned devices;
2) When viruses or malware are detected on NSU owned devices are not automatically cleaned by protection software, the device will be shut down and removed from the NSU in order for OIIT to attempt to manually remove the threats from the affected device;
3) In the event that OIIT cannot remove the infection or threat from the device, the device will be reset, reformatted, or reimaged to a new baseline configuration in order to ensure the complete removal of the infection of threat; and
4) OIIT staff will follow the Information Security Incident Response Policy regarding all threats to NSU owned devices.

- **Operating System Patches**

Almost all operating systems and many software programs have periodic security patches, released by the vendor which need to be applied. If security patches and updates are not applied on a regular basis, computer and other network devices are vulnerable to various worms, viruses, trojans, and direct malicious attacks; the result can include breach of data, denial of service, or attacks directed at other entities from the compromised device.

All NSU owned Devices, network gear, and servers are to be kept as up to date as reasonably possible with all available Operating System patches. In no circumstance will a device be allowed to remain connected to the NSU network(s) if the Operating System patches are out of data by more than 90 days, unless a documented justification is produced

to the Chief Information Officer and/or the Chief Information Security Officer and an exception granted and documented in writing. In cases where an exception is made, the device may be required to be moved to a separate part of the NSU network to isolate the device for closer monitoring for security related threats.

- **3rd Party Application Patches**

  NSU owned devices will be kept as up to date as reasonably possible with patches from 3rd party applications including, but not limited to, products as such as Adobe, Java, Hardware Drivers, etc.

  In no circumstance will a device be allowed to remain connected to the NSU network(s) if the 3rd party application patches are out of data by more than 90 days unless a documented justification is produced to the Chief Information Officer and/or the Chief Information Security Officer and an exception granted and documented in writing. In cases where an exception is made, the device may be required to be moved to a separate part of the NSU network to isolate the device for closer monitoring for security related threats.

- **Encryption**

  NSU owned devices will be required to have whole disk encryption enabled if the device supports a form of built-in or add-on software or hardware based whole disk encryption. The only allowed exception to this is for external storage devices such as USB drives, which are required to utilize encryption for any NSU data that is to be stored on these types of devices.

  All encryption products utilized on NSU owned devices shall first be vetted and approved by the Chief Information Security Officer and any encryption keys used to secure data and devices shall be stored according to guidance given by the CISO.

- **Device Firewall**

  All NSU owned devices are required to have a local device based firewall enabled if the device supports this technology. The local firewall rules will be centrally managed by the OIIT department.

- **Data Loss Prevention**

  All NSU owned devices are subject to having Data Loss Prevention (DLP) software installed to monitor and control the security, movement, removal, and disposal of NSU data.

**Violation of Policy:** If it is suspected that this policy is not being followed, report the incident to the Chief Information Security Officer.

**Policy Enforcement:** Any person found to have willfully violated this policy will be subject to appropriate disciplinary action up to and including dismissal or termination of employment.

**Timeline**

**Policy Effective Date:** Upon Implementation

**Policy Review Date:** Annually

---

**Approvals**

President & Chief Executive Officer — Date 3/30/15

Executive Vice President & Chief Operating Officer — Date 3/30/15

| APPROVED AS TO LEGAL FORM | |
|---|---|
| Signature: | |
| Print Name: | **Thomas Panza**<br>Panza, Maurer Maynard, P.A. |

| APPROVED AS TO BUSINESS CONTENT | |
|---|---|
| Signature: | |
| Print Name: | **Tom West**<br>Office of Innovation & Information Technology |