Network Security Policy

Information Technology

Purpose

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated with security threats to computing resources, and to ensure secure and reliable network access and performance for the University community. This policy is necessary to provide a reliable campus network to conduct the University's business and prevent unauthorized access to institutional, research, or personal data. In addition, the University has a legal responsibility to secure its computers and networks from misuse.

Scope

This policy applies to all Stetson University faculty, staff, students, vendors/contractors, guest account holders, and any other agents who may connect to Stetson University network computing resources. This policy also applies to all devices which are used by those individuals for network access, whether personally-owned, university-issued or otherwise obtained; and software, whether installed on Stetson devices or personally-owned devices, connected to our network; and software used to store or process Stetson University data (whether it is connected or not connected to the Stetson University network). These devices include but are not limited to workstations, laptops, tablets, smartphones, servers, consoles, controllers, and any other computing device which is capable of communicating on Stetson's networks.

Network Security Policies

1. Addressing and Domain Services

1.1. Stetson University Information Technology (SUIT) and approved administrators (Marketing and Communications) are solely responsible for managing any and all Internet domain names related to the University (e.g., stetson.edu). Individuals, academic colleges/departments or administrative departments may not create nor support additional Internet domains without prior approval from SUIT and approved administrators.

1.2. To ensure the stability of network communications, SUIT will solely provision and manage both the public and private IP address spaces in use by the University.

1.3. SUIT may delegate administrative responsibilities to individuals for certain network ranges, but retains the right of ownership for those networks.

2. Network Connections

2.1. Stetson University faculty, staff, or students may not connect, nor contract with an outside vendor to connect, any device or system to the University's networks without the prior review and approval of SUIT. Colleges or departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the University must obtain prior approval from SUIT.

2.2. In order to maintain reliable network connectivity, no other department may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus without prior review and approval of SUIT.

2.3. Users are permitted to attach devices to the network provided that they:

- are for use with normal University business or student operations
- do not interfere with other devices on the network
- are in compliance with all other Stetson policies.

2.4. Unauthorized access to University networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with University network equipment.

2.5. Unauthorized access to University equipment/cabling rooms is prohibited.

3. Wireless

3.1. SUIT is solely responsible for managing the unlicensed radio frequencies (wireless networking) on campus, which includes the 2.4 GHz and 5 GHz spectrum and may include future wireless spectrum standards, as defined by the IEEE, such as 60GHz.

3.2. SUIT is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.

3.3. The University will maintain a campus wireless network based only on IEEE 802.11 standards. SUIT will collaborate with academic departments where devices used for specific educational or research applications may require specific support or solutions.

3.4. Unauthorized devices operating in the 2.4 GHz and 5 GHz spectrums are prohibited due to interference in the operation of the Stetson University wireless network. Examples of this include but are not limited to:

- Wireless printers
- Mifi devices or wifi hotspots
- Wireless routers

4. External Traffic, Services, and Requests

4.1. The University's external Internet firewall default practice is to deny all external Internet traffic to the University's network unless explicitly permitted. To facilitate this, academic colleges/departments and other administrative departments must register systems with SUIT which require access from the Internet. Users that would like to request access through the University firewall must open a help desk ticket.

4.2. Access and service restrictions may be enforced by device, IP address, port number, or application behavior.

4.3. SUIT reserves the right to decrypt SSL traffic which transits the University network.

5. Network Security

5.1. SUIT may investigate any unauthorized access of computer networks, systems, or devices. SUIT will work with academic or administrative departments and law enforcement when appropriate.

5.2. All devices connecting to the network must have adequate security installed/maintained and must be configured and maintained in such a manner as to prohibit unauthorized access or misuse.

5.3. If a security issue is observed, it is the responsibility of all Stetson University users to report the problem to the appropriate supervisor or SUIT for investigation.

5.4. SUIT reserves the right to quarantine or disconnect any system or device from the University network at any time that is impacting regular network activity.

5.5. Network usage judged appropriate by the University is permitted. Some activities deemed inappropriate include, but are not limited to:

- Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCP or DNS servers; or a computer set up to act like such a device.
- Engaging in network packet sniffing or snooping.
- Setting up a system to appear like another authorized system on the network (trojan).

5.6. SUIT may investigate any software which is written by staff, faculty, or students that are non-commercial or not generally accepted mainstream commercial, and it is installed on university equipment or running in Stetson's network. If it does not have adequate security mechanisms, controls, and support, SUIT reserves the right to prohibit the software or system from being connected to the Stetson University network, installed on Stetson University computers, or used to store or process Stetson University data.

6. **Access Control**

6.1. Access to Stetson's resources requires a username and password. Passwords must be compliant with Stetson's Password Policy. In most cases, this policy is enforced by the system(Banner, Windows, email, etc.), however third party systems (banks, vendor accounts, etc.) must also follow the password complexity, length, and uniqueness requirements as defined in the Password Policy.

6.2. Individual user account passwords should not be shared with anyone.

6.3. Multi-Factor Authentication (MFA)

6.3.1. MFA is required by all users who access Stetson's resources to minimize the risk of compromised credentials.

6.3.2. IT recommends using "push notifications" by installing the MFA app on a smartphone.

6.3.3. Promptly report the theft or loss of a device you have configured for MFA access so IT can deactivate MFA for that device.

Enforcement

Any device found to violate this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the University's network. SUIT may subsequently require specific security improvements where potential security problems are identified before the device may be reconnected.

Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.

The University reserves the right to test and monitor security, and to copy or examine files and information resident on University systems related to any alleged security incident or policy violation.

Monitoring and Auditing

SUIT will maintain and monitor traffic logs for all network devices and systems for security auditing purposes.

SUIT reserves the right to monitor, access, retrieve, read, and/or disclose data communications when there is reasonable cause to suspect a University policy violation, criminal activity, monitoring required by law enforcement, or with appropriate management request. Reasonable cause may be provided by the complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of SUIT staff.

SUIT may perform penetration testing of any University-owned devices or systems on its networks in order to determine the risks associated with protecting University information assets. SUIT may further perform non-intrusive security audits of any system or device attached to the University's networks in order to determine what risks that system may pose to overall information security.

Questions

If you have questions or concerns regarding this policy or other Information Technology Security Policies, please contact the Office of Information Technology via phone: 386-822-7045 or email: support@stetson.edu.