Sam Houston State University
A Member of The Texas State University System
Information Technology Services (IT@Sam)

Network Use and Vulnerability Assessment Policy: IT-12

PURPOSE:

The purpose of the Network Use and Vulnerability Assessment policy is to assure the reliability, security, integrity, and availability of the telecommunications network infrastructure. This policy documents practices and responsibilities associated with the administration, maintenance, expansion, and use of the university network in order to:

1. Provide reliable network communications for the efficient conduct of university business;
2. Assure that network usage is authorized and consistent with the university's mission; and
3. Protect the confidentiality, integrity, and availability of university information that traverses the university network.

SCOPE:

The SHSU Network Use and Vulnerability Assessment policy applies equally to all individuals utilizing any Sam Houston State University information technology resources.

POLICY STATEMENT:

The Information Resources Manager (IRM) has central oversight and is responsible for the management of the SHSU network infrastructure resources. All devices connected to the SHSU network (wired or wireless) should support the university's mission. The integrity, security, and proper operation of the university network require an orderly assignment of network addresses and the correct configuration of devices attached to the network. Network access, performance, and security are put at risk when devices are introduced into the network environment without appropriate coordination.

IT@Sam will perform periodic vulnerability assessments and network scans to determine if assets hosted on SHSU's network are vulnerable to any known flaws in the operating system, services or application. The results are intended to assist server and application owners in securing their assets and any university related data that they may house. Server or Application owners will be notified of any vulnerability present on their systems, and any servers whose vulnerabilities have not been remediated in a predetermined amount of time may be disconnected from SHSU's network.

IT@Sam manages university network connections with consideration for the university mission, accessibility, performance, privacy, and security in compliance with the following:

1. No individual or university component may independently deploy network devices that extend the university network, or secure or isolate parts of the university network, except as stipulated under this policy's provisions.
2. IT@Sam is charged with overall responsibility for proper deployment and management of a fully-monitored and protected network communication service, including all infrastructure elements, network address assignments, and radio frequency (RF) spectrum usage.
3. IT@Sam shall coordinate the connection and network address assignment of any and all devices on the university network. Other departments and individual users may not install, alter, extend or re-transmit network services in any way without prior proper approval.
4. Departments and individual users are prohibited from attaching or contracting with a vendor to attach port assignable, hard-wired equipment such as routers, switches, hubs, firewall appliances, wireless access points, virtual private network (VPN) servers, network address translators, proxy servers, and dial-up servers to the university network without prior authorization from IT@Sam.
5. IT@Sam may disconnect and remove any IT@Sam unauthorized network device, including wireless routers and access points.
6. Personal software firewalls are permitted, as are printers, scanners, and similar peripheral devices if directly connected as a peripheral device to a desktop or notebook computer. IT@Sam reserves the right to monitor and audit individual devices, systems, and general network traffic to ensure compliance with this and other university policies.
7. Use of devices connected to the university network is accompanied by certain responsibilities. Specifically, all users are required to ensure timely updates of applications, operating systems, and virus protection software to minimize risks of system compromise. (IT@Sam provides non-intrusive products and services for achieving such updates.)
8. The university network is unencrypted. Server and application administrators that utilize this network to transmit sensitive, restricted and confidential information are responsible for information security on the network. Examples of available protections include encrypted protocols such as SSL, IPSec, SSH, etc. Contact IT@Sam for assistance in implementing the necessary protective measures.
9. IT@Sam requires the registration of servers connected to the university network, which must be collocated in the IT@Sam data center. Following registration, IT@Sam will facilitate an information-technology risk assessment to ensure compliance with state and university standards and best practices. A department's administrative head is responsible for designating a server administrator for each server. The server administrator shall collaborate with IT@Sam as necessary to:
    a. Register the server with the ISO;
    b. Protect the server against exploitation of known vulnerabilities.
    c. Address and resolve security problems identified with any device or application for which they are responsible.

d. Utilize the protection benefits available through the university's network edge protection mechanisms (e.g., firewall, intrusion prevention systems, etc.);
e. Accommodate risk assessments, vulnerability scans, and penetration tests of their server by IT@Sam and take steps to mitigate the risks identified by these procedures; and
f. Immediately report system compromises and other security incidents to the ISO.

10. Internet connectivity is ubiquitous across the campus. Virtually all rooms and meeting spaces at SHSU are equipped with wired or wireless connectivity. Nevertheless, facility reservations do not necessarily include the right to use the university network for any and all purposes. Consistent with IT-01, Acceptable Use policy, the university cannot guarantee support of audio or video streaming by reserving parties.

    a. Departments that accept facility reservation requests from external parties will ascertain the party's need for audio or video transmissions and consult with IT@Sam about that need. To assure compliance with this provision, departments that administer building or room reservations should include the following (or similar) statement on all reservation applications and request forms: "Streaming of audio or video is not permitted from this facility without advance notice and consultation. The reserving party declares that it – DOES / DOES NOT (circle one) – wish to stream audio or video from this facility."

DEFINITIONS:

Application Owner: The individual or group that holds ultimate responsibility for a specific service or application.

Dial-Up Server: Refers to connecting a device to a network via a modem and a public telephone network.

Encryption: The conversion of data into a form called cipher text that cannot be easily understood by unauthorized people.

Hub: A connection point for devices in a network to connect segments of a LAN.

Firewall: A network security system that controls the incoming and outgoing network traffic based on applied rule sets.

Information Resources Manager (IRM): Officer responsible to the State of Texas to manage SHSU information technology resources.

Network Address: A network address (Internet Protocol (IP) address) serves as a unique identifier for a computer on a network.

Network Address Translator: The translation of an Internet Protocol (IP) address used within one network to a different IP address known within another network.

Network Scan: The procedure for identifying active hosts on a network for network security assessments.

Penetration Test: Security oriented probing of a computer system, network or web application to seek out vulnerabilities that an attacker could exploit.

Personal Firewall: A software application used to protect a single internet-connected computer from intruders (sometimes called a desktop firewall).

Proxy Server: A server that sits between a client and an external network to allow clients to make indirect network connections to other network services.

Radio frequency (RF) spectrum: Any frequency within the electromagnetic spectrum associated with radio wave propagation.

Risk Assessment: A systematic process of identifying, evaluating, and estimating the levels of risks involved in a process or system, their comparison against benchmarks or standards, determining appropriate ways to eliminate or control the hazard, and determining an acceptable level of risk.

Router: A device, connected to at least two networks that forwards data packets from one network to another.

Server Owner: The individual or group that is responsible for managing a specific application server on a day-to-day basis.

Switch: A managed connection point for devices in a network to connect segments of a LAN.

Virtual Private Network (VPN) Server: A server that extends a private network across a public network, like the internet, to provide remote offices or individuals with secure access to the SHSU network using special hardware and software.

Vulnerability: A flaw or weakness in hardware, software or processes that exposes a system to compromise.

Vulnerability Assessment: The process of identifying, quantifying, and prioritizing the vulnerabilities (weaknesses) in a system.

Wireless Access Point: A device that allows wireless devices to connect to a wired network using Wi-Fi.

Wired Connectivity: A term used to describe any computer connection or network where the connection between sender and receiver involves cables, such as Ethernet.

Wireless Connectivity: A term used to describe any computer connection or network where there is no physical wired connection between sender and receiver.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 31, 2015
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2016