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

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

POLICY STATEMENT:

1. IT 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.

2. Information system custodians and owners will be notified of any vulnerability present on their systems, and any devices whose vulnerabilities have not been remediated in a predetermined amount of time may be disconnected from SHSU's network.

3. 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.

4. IT 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.

5. IT shall coordinate the connection and network address assignment of 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.

6. 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.

7. IT may filter, disconnect, and remove any IT unauthorized network device, including wireless routers and access points.

8. 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 reserves the right to monitor and audit individual devices, systems, and general network traffic to ensure compliance with this and other university policies.

9. Use of devices connected to the university network must include using currently supported Operating Systems and applications. In addition, users must apply security updates to Operating Systems, applications, and anti-malware software to minimize risks of system compromise.

10. Information system owners and custodians that utilize the SHSU 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 for assistance in implementing the necessary protective measures.

11. IT requires the registration of information systems (servers, network storage, etc.) connected to the university network, which must be collocated in an IT data center. Following registration, IT 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 an information system owner for each server. The information system owner shall collaborate with IT as necessary to:

    a. Register the server with the Information Security Officer (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 and take steps to mitigate the risks identified by these procedures; and
    f. Immediately report system compromises and other security incidents to the ISO.

12. 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 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 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."

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University Systems Rules and Regulations (TSUS), Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, May 2, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, May 2023
Next Review: May 2024