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

Server Administration Policy: IT-14

PURPOSE:

The purpose of this policy is to establish the framework to protect Sam Houston State University (SHSU) servers against unauthorized access, disclosure, modification, or destruction and to assure the availability, integrity, authenticity, and confidentiality of information. A server is defined as a computer system dedicated to providing services, as a host, to serve the needs of the users of other computers on the network.

This policy establishes standards for the base configuration of server equipment (physical or virtual devices), licensing, unnecessary services, default passwords, and disconnection/isolation of threatening servers that are owned and/or operated by SHSU.

SCOPE:

The SHSU Server Administration policy applies to all personnel and departments that utilize any servers or information technology resources that are owned or managed by SHSU.

POLICY STATEMENT:

All personnel and departments utilizing SHSU-owned or managed servers will comply with the procedures required in this and related SHSU policies, Texas State University System (TSUS) Rules and Regulations, and other state and federal guidelines and requirements.

PROCEDURES:

1. Server and storage information systems configuration standards and procedures are established and maintained by IT Systems and Operations and approved by the Information Security Officer (ISO).

2. All server and storage information systems must be in physically secure locations and must be safeguarded in compliance with the IT Physical Access & Environmental Policy (IT-25). Servers are specifically prohibited from operating from uncontrolled cubicle and office areas.

3. All server and storage information systems that connect to the SHSU network must be installed, configured, and managed by IT Systems and Operations.

4. All server and storage information systems must be configured to the following minimum specifications:

a. Install an appropriately licensed server operating system and antivirus protection software.
b. Make every effort to adhere to the latest applicable security configuration benchmarks published by the Center for Internet Security (CIS).
c. Disable all default accounts except those required to provide necessary services.
d. Install the most recent security patches as soon as practical according to Change Management Policy (IT-09).
e. Disable all services and applications that are not required for the server to meet its mission (e.g., Telnet, FTP, DNS, DHCP and SMTP on a file server).
f. Include the use of standard security principles of least-required access to perform a function (e.g., do not use root access when a non-privileged account will do).
g. Install appropriately licensed software required by the Data Owner or Application Administrator.
h. If a methodology for secure channel connection is necessary, privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
i. Servers must have the necessary vulnerability scans performed before providing service to the campus or internet. Any serious vulnerability must be corrected before being placed into production.
j. Those servers that house confidential university data, or that provide access to it, may be required to meet additional requirements as defined by the appropriate data owner.
k. An SHSU device registry is maintained by IT to facilitate compliance with security policies and procedures and assist in diagnosing, locating, and mitigating security incidents on the university network.
    i. Servers that attach to the SHSU network must be registered by IT and approved by the ISO.
    ii. Registration must include contact(s) and location, hardware and operating system/version, main function(s) of the server, associated applications, and demonstrated compliance.
    iii. The ISO will require the update of registry information in conjunction with the annual information security risk assessment process.

5. Information system owners and custodians must:

    a. Enforce the application's usage policies, implement the application-specified access controls, and configure and maintain the server's application according to the required standards.
    b. Include the use of standard security principles of least-required access to perform a function (e.g., do not grant an administrative account access to the application when a non-privileged account will do).

6. Backups should be completed regularly based on a risk assessment of the data and services provided and must comply with the Data Backup Policy (IT-11).

7. The ISOIT will disconnect a server or storage information system posing an immediate threat to the SHSU network to isolate the intrusion or problem and minimize risks.

    a. This can be done without contacting the owner or custodian if circumstances warrant.
    b. The server or storage information system will remain disconnected until it is brought back into compliance or is no longer a threat.

8. SHSU cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations and will file criminal complaints against users who access or utilize the network to conduct a criminal act.

    a. In accordance with the SHSU Security Incident Response Standard/Plan, incident response best practices must be followed to assure appropriate preservation and treatment of forensic data.
    b. If available, the following logs and audit trails pertaining to security-related events on critical or sensitive systems shall be maintained:
        i. Operating System Events
            1. start up and shut down of the system
            2. start up and shut down of a service
            3. network connection changes or failures
            4. changes to, or attempts to change, system security settings and controls
        ii. Operating System Audit Records
            1. log on attempts (successful or unsuccessful)
            2. the function(s) performed after logged on (e.g., reading or updating critical file, software installation)
            3. account changes (e.g., account creation and deletion, account privilege assignment)
            4. successful/failed use of privileged accounts
        iii. Application Account Information
            1. successful and failed application authentication attempts
            2. application account changes (e.g., account creation and deletion, account privilege assignment)
            3. use of application privileges
        iv. Application operations
            1. application startup and shutdown
            2. application failures
            3. major application configuration changes
            4. application transactions, for example,
                a. e-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail
                b. Web servers recording each URL requested and the type of response provided by the server
                c. business applications recording which financial records were accessed by each user
        v. The details logged for each event may vary widely, but at minimum each event should capture

1. timestamp
2. event, status, and/or error codes
3. service/command/application name
4. user or system account associated with an event
5. Device used (e.g., source and destination IPs, terminal session ID, web browser, etc.)

c. The ISO will:
   i. Perform periodic reviews to assure compliance with this policy.
   ii. Notify the Information Resources Manager (IRM) of identified concerns and risks.

9. Exceptions to the Server Administration Policy must be submitted in writing and approved by the ISO. Requests shall be justified, documented, and communicated as part of the risk assessment process.

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 TSUS Rules and Regulations, 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