

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

**Server Administration Policy: IT-14**

**Introduction:**

The purpose of this policy is to establish standards for the base configuration of server equipment (physical or virtual devices) that is owned and/or operated by SHSU. Effective implementation of this policy will minimize unauthorized access to SHSU proprietary information and technology and achieve consistency, increase availability and security, facilitate disaster recovery, coordinate technical operations and apply sound information technology management practices consistently throughout the university.

**Scope:**

The SHSU Server Administration policy applies equally to any SHSU server owners and server administrators as defined in Policy Compliance IT-00.

**Policy Statement:**

Server configuration guides must be established, maintained by each server administrator and approved by ISO. Each server owner must establish a process for changing the configuration guides, which includes review and approval by the ISO.

1. Before purchasing any equipment for use as a server, departments must contact IT@SAM to explore alternatives for centrally hosting the desired services. If adequate resources do not already exist, IT@SAM will assist the department in configuring a server adequate to address the requirements.
2. Servers must be registered by the server owner with the ISO. Registration must include contact(s) and location, a backup contact, hardware and operating system/version, main function(s) of the server, associated applications, and demonstrated compliance with the following:
  - a. IT-05 Data Access Review Policy;
  - b. IT-06 Data Classification Policy;
  - c. IT-07 Security Incident Management Policy;
  - d. IT-08 System Development Policy;
  - e. IT-09 Change Management Policy;
  - f. IT-11 Data Backup Policy;
  - g. IT-12 Network Use and Vulnerability Assessment Policy;
  - h. Other applicable SHSU policies; and
  - i. TAC 202 and other state and federal guidelines.
3. Server owners and administrators must make every effort to adhere to the latest applicable security configuration benchmarks published by the Center for Internet Security (CIS).
4. The ISO maintains a device registry to facilitate compliance with security policies and procedures and assist in diagnosing, locating and mitigating security incidents on the university network. Server owners must register their servers in this registry and maintain the accuracy of their servers' registry information. The ISO

will require the update of registry information in conjunction with the annual information security risk assessment process.

5. The server administrator of the system must install the most recent security patches as soon as practical except when immediate application would interfere with business requirements.
6. Server administrators must subscribe to vendor notification and automated update services appropriate to the software hosted on their servers. System administrators may be required to subscribe to university-provided notification and update services (or equivalent) as those services become available (e.g., System Center Configuration Manager (SCCM)).
7. Services and applications that will not be used must be disabled where practical.
8. Trust relationships between systems are a security risk and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
9. Always use 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).
10. If a methodology for secure channel connection is technically feasible, privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
11. Servers must be physically located in an access-controlled environment. Servers are specifically prohibited from operating from uncontrolled cubicle and office areas.
12. Servers that pose an immediate threat to network operations, performance, or other network-connected devices must be disconnected or quarantined to minimize risk until the threat is removed.
13. Incident response best practices must be followed to assure appropriate preservation and treatment of forensic data.
14. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - a. All security related logs will be kept online for a minimum of 1 week.
  - b. Daily incremental tape backups will be retained for at least 1 month.
  - c. Weekly full tape backups of logs will be retained for at least 1 month.
  - d. Monthly full backups will be retained for a minimum of 2 years.
  - e. Security-related incidents must be reported by the server owner or administrator to the ISO. The ISO will review logs and report incidents to the IRM. Corrective measures will be prescribed as needed. Security-related incidents include but are not limited to:
    - i. Port-scan attacks;
    - ii. Possible security breach;
    - iii. Evidence of unauthorized access to privileged accounts; and
    - iv. Anomalous occurrences that are not related to specific applications on the host.

**The ISO will:**

1. Perform periodic reviews to assure compliance with this policy.
2. Notify the Information Resources Manager (IRM) of identified concerns and risks.

**Related Policies, References and Attachments:**

An index of approved IT@SAM policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, May 15, 2011

Approved by: President's Cabinet, June 27, 2011

Next Review: November 1, 2014