**Server Management Policy UPPS No. 04.01.09**

**Issue No. 6**

**Effective Date: 07/18/2022**

**Next Review Date: 06/01/2025 (E3Y)**

**Sr. Reviewer: Associate Vice President for Technology Resources**

**POLICY STATEMENT**

*Texas State University is committed to maintaining effective, efficient, and secure management of the enterprise servers consistent with the mission and goals of the university.*

**01. SCOPE**

01.01 This policy promotes the appropriate management of university servers to achieve consistency, increase availability and security, facilitate disaster-recovery, coordinate technical operations, and apply sound information technology (IT) management practices consistently throughout Texas State University.

**02. RELATED DOCUMENTS**

02.01 [UPPS No. 04.01.01](http://policies.txstate.edu/university-policies/04-01-01.html), Security of Texas State Information Resources

02.02 [UPPS No. 04.01.05](http://policies.txstate.edu/university-policies/04-01-05.html), Network Use Policy

02.03 [UPPS No. 04.01.10](https://policies.txstate.edu/university-policies/04-01-10.html), Information Security Incident Management

02.04 [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources

**03. DEFINITIONS**

03.01 Application Administrator – the designated administrator of a hosted service. This person is the responsible party for the operation of the application.

03.02 Device Registry – a database of university network devices maintained by Information Security to assist with incident response and alerts. This registry includes information about the device such as device name, function, operating system, and primary and secondary contact information.

03.03 Hosted Service – a service hosted by Technology Resources either in the Texas State data center or in a cloud environment.

03.04 Penetration Test – evaluates the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. The intent of a penetration test is to determine the feasibility of an attack and the potential impact of a successful exploit, if discovered.

03.05 Server – a physical or virtual device that provides a specific type of service on behalf of another computer or computer user (i.e., a client). Examples include a file server that stores and manages access to files, a web server that facilitates access to websites and pages, and a name server that maps user and computer names to machine and network addresses.

03.06 Server Administrator – an individual designated by the server owner as principally responsible for performing server management functions, including the installation, configuration, security, ongoing maintenance, and registration of the server.

03.07 Server Management – functions associated with the oversight of server operations. These include controlling user access, establishing and maintaining security measures, monitoring server configuration and performance, and risk assessment and mitigation.

03.08 Server Owner – the department or unit head charged with overall responsibility for the server asset in the university’s inventory records.

03.09 Vulnerability Patch – an update provided by a vendor to correct a flaw or weakness in a component's design, implementation, or operation and management that could be exploited to violate the component's security or integrity. All software and hardware are subject to vulnerability and firmware patches.

03.10 Vulnerability Scan – a procedure that proactively identifies the vulnerabilities of a networked computing system to determine if and where that system is vulnerable to exploitation or threat. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, tests the system for these flaws, and reports the findings to improve the security of the system and the network to which the system is connected.

**04. GENERAL REQUIREMENTS**

04.01 Before connecting to the Texas State university network, servers must comply with the general requirements outlined in this policy, as well as all of the following:

1. [UPPS No. 04.01.05](http://policies.txstate.edu/university-policies/04-01-05.html), Network Use Policy (specifically, Section 04. describing the requirements for devices connecting to the university network);
2. Texas State’s [Server Management Technical and Security Standards and Procedures](https://infosecurity.txstate.edu/services-tools/security-services/server-management.html); and
3. the [Server Backup and Recovery Guide](https://infosecurity.txstate.edu/services-tools/security-services/server-management/server-backup-and-recovery-guide.html).

Server administrators must contact the IT Assistance Center (ITAC) at 512.245.ITAC (4822), or Information Security at 512.245.HACK (4225), with questions about the guidance provided in these documents.

 04.02 Server administrators shall also make every effort to adhere to the latest applicable [Security Configuration Benchmarks](http://cisecurity.org/en-us/?route=downloads.benchmarks) published by the Center for Internet Security (CIS). [CIS Benchmarks](https://www.cisecurity.org/) are provided for a wide array of operating systems, application software, and multiple versions thereof. [CIS Benchmarks](https://www.cisecurity.org/) are defined via consensus among security professionals worldwide and used by thousands of enterprises as their *de facto* local configuration standards. Contact Texas State’s Information Security team (infosecurity@txst.edu) for assistance in utilizing these benchmarks.

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

04.04 The server owner is responsible for the management, operation, and security of the server. At a minimum, the owner must assure the following:

1. the server is registered in the device registry described in Section 04.03;
2. physical and network access to the server is properly controlled; and
3. the server’s operational configuration is maintained within the security and operational parameters described in this policy.

The owner may delegate specific server management responsibilities to a server administrator to achieve these objectives, but the server owner retains ultimate responsibility.

04.05 Before purchasing any equipment for use as a server, departments should contact ITAC to explore alternatives for centrally hosting the desired services. If adequate resources do not already exist, Technology Resources will assist the department in configuring a server adequate to address the requirements.

04.06 System owners and administrators shall adhere to the provisions of Section 02.10 of [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources, when transferring, repurposing, destroying, or otherwise disposing of their server.

04.07 System 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).

04.08 Hosted services are provided by Technology Resources after a review by the Information Security Office and must have a data security plan in place before any services will be provided.

04.09 Application administrators of a hosted service are responsible for the data and administration of the application and any dependencies. Technology Resources has posted [Server Admin Guidelines](https://itac.txstate.edu/support/servers/server-admin-guidelines) that all application administrators must follow and details the responsibilities of both parties.

04.10 It is not possible for this policy to address every specific issue that may arise regarding server management at Texas State. Server owners and administrators are expected and encouraged to seek guidance from ITAC, which will involve other components of the IT division as necessary to meet these responsibilities.

04.11 Exceptions to this policy require collaboration with Technology Resources and the Information Security Office, as well as the express permission from the associate vice president for Technology Resources, or designee.

**05. PROCEDURES FOR RESPONSE TO THREATS AND POLICY VIOLATIONS**

 05.01 Texas State’s Information Security team employs a variety of techniques

and technologies, including regular network vulnerability scans and penetration tests, to identify potential risks to campus information resources and to monitor compliance with this policy. Information Security will notify the registered server administrator of any protection deficiencies discovered in the course of these activities and recommend options for eliminating the deficiencies. If the deficiencies are not corrected or the server remains out of compliance for three or more calendar days following notification, Information Security may, with the concurrence of the Information Security officer or the associate vice president for Technology Resources, disable the server’s connection to the university network until the deficiency is remedied.

 05.02 In emergency circumstances, Information Security will attempt to notify

the server owner or administrator whenever it determines that a server has become an imminent threat to university information resources, such as when a server’s integrity is compromised, when it places other network users at risk, or when its defenses against compromise are seriously inadequate for the purpose it serves. If Technology Resources or Information Security cannot contact the server administrator or the administrator does not respond in a timely manner, Information Security may isolate the offending server from the network until the risk is mitigated. If the threat results in the inappropriate disclosure of sensitive or restricted and confidential information, Information Security will initiate the incident management procedures located in [UPPS No. 04.01.10](https://policies.txstate.edu/university-policies/04-01-10.html), Information Security Incident Management.

**06. REVIEWERS OF THIS UPPS**

06.01 Reviewers of this UPPS include the following:

Position Date

Associate Vice President for June 1 E3Y

Technology Resources

Chief Information Security Officer June 1 E3Y

Director, Network Operations June 1 E3Y

**07. CERTIFICATION STATEMENT**

This UPPS has been approved by the following individuals in their official capacities and represents Texas State policy and procedure from the date of this document until superseded.

Associate Vice President for Technology Resources; senior reviewer of this UPPS

Vice President for Information Technology

President