TEXAS SOUTHERN UNIVERSITY

MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **NUMBER: 04.06.24**
AREA: Computer and Information Technology

TITLE/SUBJECT: Server Hardening Policy

I. POLICY STATEMENT

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

II. PURPOSE AND SCOPE

The purpose of the Server Hardening Policy is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

The Server Hardening Policy applies to all individuals that are responsible for the installation of new Information Resources, the operation of existing Information Resources, and individuals charged with Information Resource Security.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

1. A server must not be connected to the University network until it is in an Office of Information Technology ("OIT") accredited secure state and the network connection is approved by OIT.

2. The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for OIT accreditation. Some of the general steps included in the Server Hardening Procedure are:

    2.1. Installing the operating system from an IS approved source.

    2.2. Applying vendor supplied patches.

2.3. Removing unnecessary software, system services, and drivers.

2.4. Setting security parameters, file protections and enabling audit logging.

2.5. Disabling or changing the password of default accounts.

3. OIT will monitor security issues, both internal to the University and externally, and will manage the release of security patches on behalf of the University.

3.1. OIT will test security patches against OIT core resources before release where practical.

3.2. OIT may make hardware resources available for testing security patches in the case of special applications.

3.3. Security patches must be implemented within the specified timeframe of notification from the OIT.

4. Disciplinary Action

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 – Discipline and Termination Policy).

5. Applicable TSU Security Policy Standards

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 8
- Security Standard 11
- Security Standard 12
- Security Standard 16
- Security Standard 17

6. Review and Responsibilities

Responsible Party: Chief Information Officer

Review: Every 3 years, on or before September 1st

Forms

None

V. APPROVALS

Chief Information Officer

President

Effective Date 2/1/2018