TEXAS SOUTHERN UNIVERSITY

MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: **Information Technology** **NUMBER:** **04.06.16**
AREA: **Computer and Information Technology**

TITLE/SUBJECT: **Network Port Scanning Policy**

I. POLICY STATEMENT

Port scanning should be done as means to assess TSU information resources and technology vulnerabilities. The process of sending data packets over the network to selected service port numbers (HTTP-80, Telnet-23, etc.) of a computing system with the purpose of identifying available network services on that system. This process is helpful for troubleshooting system problems or tightening system security. Network port scanning is an information gathering process, when performed by unauthorized individuals it is considered a prelude to attack.

.

II. PURPOSE AND SCOPE

Network Port Scanning should only be done under specific circumstances with proper approval. Network Port Scanning is prohibited unless written permission is provided by the Information Security Officer. The approval document will include specific parameters, restrictions, and time period during which the scan(s) may be performed with an audit trail. Any additional scanning shall require separate written approval. To the extent this policy conflicts with an existing University policy, the existing policy is superseded.

The Network Port Scanning Policy applies equally to all individuals with authorized access to any TSU Information Resource, including staff, faculty, students, consultants, contractors and volunteers.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

1. It is the policy of the Texas Southern University that no computer system connected to the University's network shall be used to perform port mapping or vulnerability scanning of Texas Southern University's information systems infrastructure without prior written consent of the Information Security Officer. Port mapping or vulnerability scanning on any computer system (including internal and external systems) shall only be performed under the following

conditions:

The Information Security Team can perform a port map or scan to monitor compliance with University policy. Scans may be performed for the purpose of security assessments, or to investigate security incidents and reporting significant findings to appropriate University Assurance functions.

2. Disciplinary Action

Violation of this policy may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline & Termination Policy).

3. 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 5
- Security Standard 6
- Security Standard 7
- Security Standard 8
- Security Standard 11
- Security Standard 12
- Security Standard 14
- Security Standard 15
- Security Standard 16
- Security Standard 17
- Security Standard 20
- Security Standard 23

4. 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