TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

**SECTION: Information Technology** **Policy 04.06.26**
**AREA: Information Security**

**SUBJECT: Technical Monitoring Policy**

## I. INTRODUCTION

The Technical Monitoring Policy goal is to ensure a reasonable expectation of privacy is given to users of TSU's Information Resources. Monitoring can and will be done under the appropriate and necessary circumstances. Targeted monitoring will be done with the prior approval from the University President, Chief Information Officer, and Information Security Officer.

## II. PURPOSE & SCOPE

The purpose of this policy is to outline TSU's guidelines regarding the monitoring, logging, and retention of network traffic being transported across the university's networks. Texas Southern University ensures that reasonable actions are being taken to assure the integrity of private and confidential electronic information transported over its networks. The goal of this policy is to maintain the confidentiality, integrity, and availability of the university's network infrastructure and information assets. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by university policies. To the extent this policy conflicts with an existing University policy, the existing policy is superseded. The Technical Monitoring Policy applies equally to all individuals with authorized access to any TSU Information Resource, including staff, faculty, students, consultants, contractors and volunteers.

## III. POLICY

A. The TSU Networking Group is authorized to monitor TSU's networking environment for routine maintenance purposes. The Information Security Team is authorized to monitor TSU's networking environment for assessment or investigative purposes. Both groups are required to obtain prior approval from the Chief Information Officer and continuous monitoring by the Information Security Officer to perform more specific monitoring of traffic or specific range of addresses.

B. Staff with authorization to monitor is limited to monitoring to detect, know patterns of attack or compromise, the improper release of confidential employee or student data, or to troubleshoot and analyze network-based problems. Routine monitoring must be held to a specific limited scope.

C. No authorized personnel shall use network monitoring devices to monitor employee electronic transmissions for job performance evaluation, or as part of an unofficial investigation, without first receiving signed approval from the President and the Office of General Counsel.

D. All monitoring must be documented with proper audit trail to the Information Security Officer's satisfaction. All approval documents and logs must be stored for future reference.

## IV. DISCIPLINARY ACTION

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

## V. 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 1
- Security Standard 5
- Security Standard 6
- Security Standard 7
- Security Standard 12
- Security Standard 16
- Security Standard 17
- Security Standard 23

## VI. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every year, on or before September 1

## VII. APPROVAL

Jim McShan

Vice President of Finance

Joe Ludley

President

2/18/11

Effective Date