TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **Policy 04.06.21**
AREA: Information Security

SUBJECT: Security Monitoring Policy

I. PURPOSE

The purpose of the Security Monitoring Policy is to ensure that information resource and technology security controls are in place, are effective and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done or to at least minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

II. SCOPE

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

A. Automated intrusion detection system logs;
B. Firewall logs;
C. User account logs;
D. Network scanning logs;
E. Application logs;
F. Data backup recovery logs;
G. Help Desk Logs, and
H. Other log and error files.

III. OWNERSHIP AND RESPONSIBILITIES

The Security Monitoring Policy applies to all individuals who are responsible for the installation of new Information Resources, the operations of existing Information Resources, and charged with Information Resource Security.

IV. POLICY PROVISIONS

A. Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and

the tools will report exceptions. These tools will be deployed to monitor:

1. Internet traffic;
2. Electronic mail traffic;
3. LAN traffic, protocols, and device inventory; and
4. Operating system security parameters.

B. The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

1. Automated intrusion detection system logs;
2. Firewalls logs;
3. User account logs;
4. Network scanning logs;
5. System error logs;
6. Application logs;
7. Data backup and recovery logs;
8. Help desk trouble tickets;
9. Telephone activity – Call Detail Reports; and
10. Network printer and fax logs.

C. The following checks will be performed at least annually by assigned individuals:

1. Password strength;
2. Unauthorized network devices;
3. Unauthorized personal web servers;
4. Unsecured sharing of devices;
5. Unauthorized modem use; and
6. Operating system and software licenses.

D. Any security issues discovered will be reported to the Information Security Officer for follow-up investigation.

V. DISCIPLINARY ACTION

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

VI. 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 16
- Security Standard 17

VII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer Billy Rutter

Review: Every year, on or before September 1

VIII. APPROVAL

Jimi McStan
Vice President of Finance

Joe Lindley
President

2/18/11
Effective Date