I. POLICY STATEMENT

Texas Southern University ("University") shall implement continuous security monitoring capabilities to proactively detect, analyze, and respond to potential security threats across all University information systems and services, including cloud, on-premises, and hybrid environments. This policy establishes that:

- Continuous monitoring of networks, systems, endpoints, applications, cloud services, and critical infrastructure is performed to identify suspicious activities, policy violations, or anomalous behavior.
- Real-time alerts and structured incident responses shall be implemented to minimize the impact of security events.
- Monitoring activities shall support compliance with applicable legal, regulatory, and contractual requirements.
- Security metrics and data-driven insights shall be utilized to enhance threat detection and defenses, and strengthen the University's overall security posture.
- Monitoring includes both automated tools and human oversight processes to ensure accuracy, completeness, and timely response. Monitoring practices shall align with risk-based controls and security standards established under the Texas Administrative Code, Title 1, Chapter 202.

Monitoring activities shall be conducted solely for legitimate institutional purposes, including security, compliance, legal obligations, and operational integrity. Access to information obtained through monitoring, including information that may constitute education records shall be limited to individuals with a legitimate educational or business interest, in accordance with applicable federal and state law.

Monitoring practices shall align with risk-based controls and security standards established under Texas Administrative Code Chapter 202.

II. PURPOSE AND SCOPE

The purpose of this Information Technology (IT) Security Monitoring Policy is to ensure that University information resources are protected through effective security controls and that threats, vulnerabilities, and policy deviations or vulnerabilities are identified and addressed in a timely manner. Security monitoring enables detection of threats or security weaknesses, minimizing potential operational impact to the University. Security monitoring supports the following objectives:

- Early detection and mitigation of security incidents
- Compliance with audit, legal, and regulatory requirements
- Service level monitoring and performance measurement
- Protection of institutional data and reduction of liability risk

This policy governs all University systems, networks, devices, applications, and information resources, regardless of location or ownership, including cloud-based and third-party managed services. It applies to all University employees, contractors, vendors, and any individual or entity with access to University information systems or data.

This policy applies to all individuals with access to University information resources, including staff, faculty, students, contractors, consultants, visitors, and volunteers.

Monitoring activities include, but are not limited to:

1. Automated intrusion detection and prevention logs;
2. Firewall and network device logs;
3. User account and authentication logs;
4. Network traffic and vulnerability scanning logs;
5. Application and system error logs;
6. Data backup and recovery logs;
7. Help Desk and incident ticketing logs;
8. Cloud service audit and activity logs;
9. Telephony, printer, and multifunction device logs;

III. POLICY PROVISIONS

1. **Automated Monitoring:** Automated and centralized monitoring tools must provide real-time alerts for detected incidents or suspicious activity. Where feasible, a security baseline will be established, and deviations will be reported. These tools will monitor:
    1.1. Internet and network traffic, including LAN, WAN, and wireless networks;

    1.2. Email systems, including cloud-based email services;

    1.3. Device inventory, endpoint configurations, and protocol usage;

    1.4. Operating system and application security parameters.

2. **Log Monitoring and Review:** System and security logs shall be reviewed at a frequency determined by risk assessment to detect signs of unauthorized activity, security incidents, or vulnerability exploitation.

   The following logs shall be reviewed:

   2.1. Intrusion detection and prevention system logs;

   2.2. Firewall and network device logs;

   2.3. User authentication and account activity logs;

   2.4. Network scanning and vulnerability assessment logs;

   2.5. System and application error logs;

   2.6. Backup and recovery verification logs;

   2.7. Help desk and incident ticket logs;

   2.8. Cloud service audit logs;

   2.9. Telephony / call detail records

   2.10. Network printer and multifunction device logs.

3. **Security Control Assessments**: Assigned personnel must perform the following checks at least annually:

   3.1. Password strength and multi-factor authentication compliance;

   3.2. Detection of unauthorized network devices;

   3.3. Detection of unauthorized web servers or services;

   3.4. Verification of secure sharing configurations;

   3.5. Unauthorized modem or network device usage;

3.6. Verification of operating system and software licensing

3.7. Review of cloud service configuration and access permissions

4. **Privacy and Data Protection**: Monitoring shall be conducted in a manner that is reasonable, proportionate, and consistent with applicable state and federal privacy protections. Special care shall be taken when monitoring systems that contain protected data, including education records, health information, and financial data.

5. **Incident Reporting:** Any security issues detected must be reported to the **Information Security Officer (ISO)** for investigation, mitigation, and documentation.

.

6. Disciplinary Action: Violation of this policy may result in immediate disciplinary action including termination, in accordance with University policy (MAPP 02.05.03 – Discipline & Termination Policy).

7. **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