I. POLICY STATEMENT

Texas Southern University ("TSU" and "the University") provides information resources to support the university's mission of teaching, research, and service. To protect these assets and ensure compliance with state and federal law, this policy establishes the limits of privacy for all users. While the University respects the privacy of its community, internal and external users have a limited expectation of privacy in University information resources, subject to applicable federal and state law and the University's need to monitor systems for legitimate business, security, and compliance purposes. The University reserves the right to monitor, access, and disclose any information processed through its systems to ensure security, compliance, and operational continuity for legitimate institutional purposes, including security, compliance, legal obligations, and operational integrity.

II. PURPOSE AND SCOPE

The purpose of this policy is to communicate the University's expectations regarding the privacy of information resources and technology. This policy applies to all individuals, including faculty, staff, students, contractors, and guests, who access or use any University information resource, regardless of location or device ownership. This policy shall be interpreted in conjunction with other applicable University policies and governing federal and state law. In the event of a conflict between this policy and any other institutional policy regarding the **use, monitoring, or privacy of information resources**, this policy shall be interpreted in conjunction with applicable federal and state laws and other University policies governing specific categories of data.

III. DEFINITIONS

1. Information Resources: All computer hardware, software, networks, systems, and data owned, operated, or maintained by the University.

2. Ownership: **All** electronic files and data created, sent, received, or stored on University-managed systems or computers owned, leased, administered, or otherwise under the custody and control of the University are the property of the University and the State of Texas.

3. Internal User: Any individual with a primary affiliation with the University, including faculty, staff, and students, who has been granted authorized access to University information resources.

4. External User: Any individual or entity without a primary affiliation with the University, authorized to access University information resources, including, but not limited to, contractors, vendors, consultants, volunteers, and guests.

IV. POLICY PROVISIONS

1. **Institutional Access:** Electronic files created, sent, received, or stored on owned, leased, administered, or otherwise under the custody and control of the University are not private. The University, through the Office of Internal Audit, the Office of Information

Technology (OIT), or the **Office of General Counsel,** reserves the right to access such files and data at any time, for any purpose, and without prior knowledge of or notice to the information resource user or owner.

2. **System Monitoring:** To maintain system integrity and security, the University may log, review, and otherwise utilize any information stored on or passing through its information resource systems. This includes, but is not limited to, web traffic, application usage, and communication metadata, in accordance with **Texas Administrative Code (TAC) 202**. For these same purposes, the University may also capture user activity, such as telephone numbers dialed and web sites visited.

3. **Regulatory Compliance:** A wide variety of third parties have entrusted their information to the University for business purposes, and all workers at the University must do their best to safeguard the privacy and security of this information. Authorized access to information resources shall be limited to authorized users based on role, job responsibilities, and the principle of least privilege. Customer account data is confidential, and access will be strictly limited based on business need for access. Users must handle all data in accordance with applicable federal and state protections, including but not limited to:

   1. FERPA: Protection of student educational records.
   2. HIPAA: Protection of health information.
   3. GLBA/PCI-DSS: Protection of financial and credit card data

4.
User Responsibilities: Users must respect the privacy of others and shall not attempt to access data for which they do not have explicit authorization. Users must immediately report any security weaknesses or potential breaches including incidents of possible misuse or violation of this agreement to the Information Security Officer (ISO).

5. **Unauthorized Access:** Users must not attempt to access any data or programs contained on University systems for which they do not have authorization or explicit consent.

6. **Web Privacy and Public Disclosure:** The University maintains a publicly accessible web privacy statement that describes the categories of information collected through its websites, the purposes for which such information is used, and any applicable use of cookies or third-party analytics tools.

Information may be subject to disclosure under the Texas Public Information Act unless expressly protected by state or federal law.

The University manages and safeguards information in accordance with applicable federal and state laws, including the Family Educational Rights and Privacy Act (FERPA), and applicable cybersecurity standards under Texas Administrative Code Title 1, Chapter 202, as well as institutional policies and procedures.

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

8. **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 2
- Security Standard 8
- Security Standard 16