I. POLICY STATEMENT

The Texas Southern network infrastructure is provided and maintained as a central institutional utility supporting all users of Texas Southern University ('University') information resources. The Texas Southern University network, including wired and wireless connections, routers, switches, firewalls, access points, and associated systems, must support current and emerging technologies while maintaining flexibility to meet the University's evolving needs.

The network must remain secure, reliable, and capable of supporting high-speed connections, cloud services, and advanced user applications, while safeguarding the confidentiality, integrity, and availability of University resources. The University shall implement appropriate controls to prevent unauthorized access, disruption, or misuse.

II. PURPOSE AND SCOPE

The purpose of the Network Access Policy is to establish the rules governing access to and use of the University network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of the University's network and information resources. Network access shall be granted based on role, job responsibilities, and the principle of least privilege. To the extent this policy conflicts with existing University policy, this policy shall be interpreted in conjunction with applicable federal and state law and other University policies governing information security and privacy. The Network Access Policy applies equally to all individuals with access to the network or any University information resource.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

1. Users are permitted to use only those network addresses issued to them by the Office of Information Technology ("OIT").

   All remote access to University resources must occur via approved Virtual Private Network (VPN) solutions or secure protocols defined by the University. Users must authenticate using University-approved methods, including multi-factor authentication where required.

2. Remote users may connect to University information resources and technology only through University-approved channels, including VPN or equivalent secure access technologies and using protocols approved by the University. Devices connecting to the University network must meet minimum security standards, including current patching, antivirus protection, and compliance with University security configurations

3. Users inside the University firewall may not be connected to the University network at the same time a modem is being used to connect to an external network.

4. Users may not install or connect routers, switches, hubs, wireless access points, or any device that extends the University network without prior OIT approval.

5. Users may not install network hardware or software that provides network services without prior OIT's approval. Non-University computer systems that require network connectivity must conform to Texas Southern University standards.

6. Users may not run programs or tools that test, bypass, or compromise network security, including password crackers, packet sniffers, port scanners, or network mapping software, unless explicitly authorized for security testing by OIT.

7. Users may not alter, remove, or tamper with University network hardware.

8. User access shall be provisioned, modified, and revoked in accordance with University identity and access management procedures

9. Disciplinary Action

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

10. Applicable TSU Security Policy Standards

    All individuals with authorized access to any Texas Southern University 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 3
    - Security Standard 5
    - Security Standard 7
    - Security Standard 20