TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

**SECTION: Information Technology** **Policy 04.06.14**
**AREA: Information Security**

**SUBJECT: Network Access Security Policy**

## I. INTRODUCTION

The Texas Southern University ("TSU") network infrastructure is provided as a central utility for all users of University information resources. It is important that the infrastructure, which includes cabling and the associated —active equipment, continues to develop with sufficient flexibility to meet the University's demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

## II. PURPOSE & SCOPE

The purpose of the Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of the University's network resources. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Network Access Policy applies equally to all individuals with access to the network or any University information resource.

## III. POLICY PROVISIONS

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

B. All remote access (dial-in services) to TSU will be either through an approved modem pool or via an Internet Service Provider (ISP).

C. Remote users may connect to University information resources and technology only through an ISP and using protocols approved by the University.

D. 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.

E. Users must not extend or re-transmit network services in any way. This means you may

not install a router, switch, hub, or wireless access point to the University's network without OIT approval.

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

G. Users may not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, University users may not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the University's network infrastructure.

H. Users are not permitted to alter network hardware in any way.

## 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 3
- Security Standard 5
- Security Standard 7
- Security Standard 20

## VI. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every year, on or before September 1

## VII. APPROVAL

Jeri McShan

Vice President of Finance

President

2/18/11

Effective Date