TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology **Policy 04.06.15**
AREA: Information Security

SUBJECT: Network Configuration Policy

I. INTRODUCTION

The University network infrastructure is provided as a central utility for all users of University information resources and technology. It is important that the infrastructure, which includes cabling and the associated equipment, such as routers and switches, continues to develop with sufficient flexibility to meet user 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 Configuration Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of University information. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Network Configuration Policy applies equally to all individuals with access to any University information resources.

III. NETWORK CONFIGURATION SECURITY PRACTICE STANDARDS

A. The State of Texas owns the University's network infrastructure, and the Office of Information Technology ("OIT) is responsible for managing further developments and enhancements to this infrastructure.

B. To provide a consistent University network infrastructure capable of exploiting new networking developments, all cabling must be installed by OIT or an approved contractor.

C. All network connected equipment must be configured to a specification approved by OIT.

D. All hardware connected to the University network is subject to the University's information technology management and monitoring standards.

E. Changes to the configuration of active network management devices must not be made without the approval of OIT.

F. The University network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by OIT.

G. The networking addresses for the supported protocols are allocated, registered and managed centrally by OIT.

H. All connections of the network infrastructure to external third party networks are the responsibility of OIT. This includes connections to external telephone networks.

I. The information technology firewalls must be installed and configured following Firewall Implementation Standard documentation.

J. The use of departmental firewalls is not permitted without the written authorization of OIT.

K. Users must not extend or re-transmit network services in any way. This means a User may not install a router, switch, hub, or wireless access point to the University network without OIT approval.

L. Users may not install network hardware or software that provides network services without OIT approval.

M. 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 12
- Security Standard 15
- Security Standard 19
- Security Standard 20

VI. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

Review: Every year, on or before September 1

VII. APPROVAL

Vice President of Finance

President

2/18/11

Effective Date