SECTION: Information Technology **Policy 04.06.12**
AREA: Information Security

SUBJECT: Internet Use Policy

I. PURPOSE & SCOPE

Under the provisions of the Information Resources Management Act, Texas Gov. Code Chapter 2054, information resources and technology are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established:

A. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources,
B. To establish prudent and acceptable practices regarding the use of the internet, and
C. To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Internet Use Policy applies equally to all individuals granted access to any University information resource and technology with the capacity to access the internet, the intranet, or both.

II. OWNERSHIP

Electronic files created, sent, received, or stored on 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.

III. PRIVACY

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the University, are not private and may be accessed by the Office of Internal Audit or Office of Information Technology ("OIT") employees at any time without the knowledge of or notice to the information resource and technology user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

IV. INCIDENTAL USE

A. Incidental personal use of Internet access is restricted to University-approved users; it does not extend to family members or acquaintances.
B. Incidental use must not result in direct costs to the University.
C. Incidental use must not interfere with the normal performance of an employee's work duties.
D. No files or documents may be sent or received that may cause legal liability for or embarrassment to the University.
E. Storage of personal files and documents within the University's information resources and technology should be nominal.
F. All files and documents, including personal files and documents, are owned by the University, may be subject to open records requests, and may be accessed in accordance with this policy and any other applicable University policy.

V. POLICY PROVISIONS

A. Software for browsing the Internet is provided to authorized users for business and research use only.
B. All software used to access the Internet must be part of the University standard software suite or approved by OIT. This software must incorporate all vendor provided security patches.
C. All files downloaded from the Internet must be scanned for viruses using the approved OIT distributed software suite and current virus detection software.
D. All software used to access the Internet shall be configured to use the firewall http proxy.
E. All sites accessed must comply with the University's Computer Use Policy (MAPP 04.06.03) and all other relevant information technology policies.
F. All user activity is subject to logging and review.
G. Content on all University web sites must comply with the University's Computer Use Policy (MAPP 04.06.03) and all other relevant information technology policies.
H. No offensive or harassing material is permitted on University web sites.
I. No personal commercial advertising is permitted on University web sites.
J. University internet access may not be used for personal gain or non-University personal solicitations.
K. No University data will be made available via University web sites without ensuring that the material is available to only authorized individuals or groups.
L. All sensitive or confidential University material or data transmitted over external network must be encrypted.
M. Electronic files must be retained in accordance with state law and/or University policy.

VI. DISCIPLINARY ACTION

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

VII. 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 3
- Security Standard 6
- Security Standard 7
- Security Standard 16

VIII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer Billy Rector

Review: Every year, on or before September 1

IX. APPROVAL

Jim McShan
Vice President of Finance

President

2/18/11
Effective Date