



**TEXAS SOUTHERN UNIVERSITY**  
**MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES**

**SECTION: Information Technology**  
**AREA: Information Security**

**Policy 04.06.23**

<b>SUBJECT: Security Training Policy</b>
--

### **I. INTRODUCTION**

Information Security Awareness training provides a method of educating and fostering accountability for use of Information Resources. Educating all users on regulation, standards, and best practices is vital to any information security program.

### **II. PURPOSE & SCOPE**

The purpose of the Security Training Policy is to describe the requirements to ensure each user of Information Resources receives adequate training on computer security issues. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Security Training Policy applies equally to all individuals who use any University Information Resources.

### **III. POLICY PROVISIONS**

- A. All new users must attend an approved Security Awareness training class prior to or at least within thirty (30) days of being granted access to any University Information Resources. The training may be included as part of the new employee orientation that all employees are required to attend.
- B. All users must sign an acknowledgement stating they have read and understand the University's computer security policies and procedures.
- C. All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect the University's information resources.
- D. The Office of Information Technology ("OIT") must prepare, maintain, and distribute one or more Information Security Hand-outs that concisely describe the University's information security policies and procedures.
- E. All users must attend information security awareness training annually and fulfill all requirements associated with the training.

- F. OIT must develop and maintain a communications process to for communicating new computer security program information, security bulletin information, and security items of interest.

**IV. DISCIPLINARY ACTION**

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 – Discipline & 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 2
- Security Standard 3

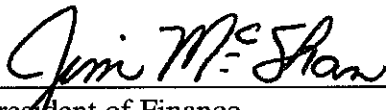
**VI. REVIEW AND RESPONSIBILITIES**

Responsible Party: Chief Information Officer

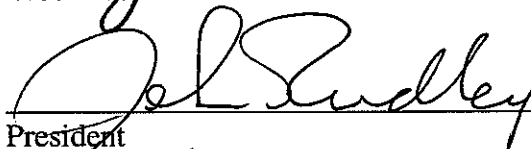


Review: Every year, on or before September 1

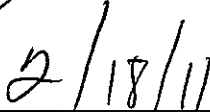
**VII. APPROVAL**



Vice President of Finance



President



Effective Date