TEXAS STATE TECHNICAL COLLEGE

# STATEWIDE OPERATING STANDARD

| | | |
|---|---|---|
| **No. GA 5.1.8** | **Page 1 of 3** | **Effective Date: 4/04/2019** |
| **DIVISION:** | **General Administration** | |
| **SUBJECT:** | **Information Security Awareness and Training** | |
| **AUTHORITY:** | **Statewide Operating Standard GA 5.1** | |
| | | |
| **PROPOSED BY:** | **Shelli Scherwitz** | |
| **TITLE:** | **Executive Vice President of Information Technology** | **Date: 4/04/2019** |
| | | |
| **RECOMMENDED BY:** | **Rick Herrera** | |
| **TITLE:** | **Vice Chancellor & Chief Student Services Officer** | **Date: 4/04/2019** |
| | | |
| **APPROVED BY:** | **Mike Reeser** | |
| **TITLE:** | **Chancellor** | **Date: 4/04/2019** |

**STATUS:** Approved by LT 4/04/2019

**HISTORICAL STATUS:** Approved by LT 5/26/2017
Proposed 5/11/2017
New 3/22/2017

## I. STATEWIDE STANDARD

EXECUTIVE ORDER: By order of the Chancellor, Texas State Technical College (TSTC) shall establish standing orders, as necessary, to implement the directive of the Board of Regents to secure the College's information technology resources.

## I. PERTINENT INFORMATION

Under the provisions of the Texas Government Code, Title 10, Subtitle B, Chapter 2054, Subchapter A, information resources are strategic assets of TSTC that must be managed as valuable resources.

## II. GENERAL GUIDELINES

This Statewide Operating Standard (SOS) shall establish the rules regarding information security awareness and training which must be implemented to achieve the following:

1. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
2. To ensure compliance with prudent and acceptable practices regarding the use and security of information resources.

## III. DEFINITIONS

**FERPA-Protected Information:** Any student data elements that TSTC has not determined to be directory information as per the College's SOS GA 1.5.2 Student Records and the Family Educational Rights Privacy Act (FERPA). For additional detail see SOS GA 5.1.6 Data Classification and Handling Standard.

**Information Resources:** Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data to include, but is not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network-attached and computer-controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus, as well as the procedures, equipment, facilities, and software. Also included are devices, programs, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information on those resources.

## IV. DELEGATION OF AUTHORITY

The Chancellor has the authority to implement this SOS and delegates to the appropriate Vice Chancellor the responsibility to deploy resources, processes, and procedures to ensure compliance with this standard and any applicable federal, state, and/or local regulations.

## V. PERFORMANCE STANDARDS

1. All College personnel who may access or utilize TSTC information resources are provided with periodic training in information security and awareness.

2. All College personnel who may access or utilize TSTC information resources do so in accordance with SOS GA 5.1.4 Acceptable Use of Information Technology Resources.

# APPENDIX

## VI. RELATED STATEWIDE STANDARDS, LEGAL CITATIONS, OR SUPPORTING DOCUMENTS

Family Educational Rights Privacy Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C
GA 1.5.2 Student Records
GA 5.1.4 Acceptable Use of Information Technology Resources
GA 5.1.6 Data Classification and Handling Standard
HR 2.4.1 Employee Corrective Action

## VII. OPERATING REQUIREMENTS

1. All users of TSTC information technology must undergo annual fundamental information technology security awareness and training. The fundamental training shall ensure that users are fully informed of policies, procedures, and rules related to information technology security at the time of hire and on an annual basis. The training must be designed to ensure that:
   a. Users are fully informed of common threats such as phishing, malware, and social engineering;
   b. Users are fully informed of data classification and handling requirements such as FERPA;
   c. Users are fully informed of fundamental network and workstation acceptable use expectations;
   d. Users are aware of how to identify and report potential internal threats where a user is attempting to exceed or abuse authorized access; and
   e. Users are fully informed of how to identify and report security incidents as appropriate.

   In addition to the fundamental annual security awareness and training program, the Office of Information Technology shall periodically engage users across the College regarding new threats and periodic awareness reminders.

2. In addition to basic annual user training, users in various areas of the College may be required to take additional training appropriate for unique threats and requirements in the context of their level of access and functional area.

3. As part of the training process for all users and privileged users, records of training attempts shall be stored. In the event of incomplete training, employees and their supervisors shall be notified.

4. Non-compliance with established standards, rules, and procedures regarding information security and use of information technology shall subject an employee to a range of corrective actions pursuant to the College's SOS HR 2.4.1 Employee Corrective Action.