TEXAS STATE TECHNICAL COLLEGE

STATEWIDE OPERATING STANDARD

No. GA 5.1	**Page 1 of 4**	**Effective Date: 01/22/2019**
DIVISION:	**General Administration**	
SUBJECT:	**Information Technology**	
AUTHORITY:	**Minute Order #21-13**	
PROPOSED BY:	**Shelli Scherwitz**	
TITLE:	**Senior Executive Director - Information Technology**	**Date: 01/22/2019**
RECOMMENDED BY:	**Rick Herrera**	
TITLE:	**Vice Chancellor/Chief Technology Officer**	**Date: 01/22/2019**
APPROVED BY:	**Mike Reeser**	
TITLE:	**Chancellor**	**Date: 01/22/2019**

STATUS: Approved by LT 01/22/2019

HISTORICAL STATUS: Approved by LT 4/12/2018
Approved by EMC 6/09/2015
Revised 04/2015
Reviewed 6/2014
Approved by BOR 2//7/13
Original Proposed 2/7/13
Formerly Titled: Information Technology Resource Management

I. STATEWIDE STANDARD

POLICY: It is the policy of Texas State Technical College (TSTC) that the College effectively and efficiently govern information technology resources in a manner that supports the goals and objectives of the College; considers applicable regulations, guidelines, standards, and best practices; and supports practices that result in the protection, availability, and security of technology assets and data.

II. PERTINENT INFORMATION

Because information resources owned and operated by TSTC are valuable assets to the operation and mission of the College, measures to protect those resources are both necessary and prudent. Commensurate with the value of the asset, measures should include guidelines to protect against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate. Additionally, measures should ensure the availability, integrity, utility, authenticity, and confidentiality of information.

III. GENERAL GUIDELINES

This Statewide Operating Standard (SOS) regarding information technology shall establish the principles, rules, and procedures applying to all members of the TSTC community to address issues particular to the use of electronic communications. Security requirements shall be identified, documented, and addressed in all phases of development and/or acquisition of information resources. TSTC policies shall clarify the applicability of law to electronic communications and shall reference other TSTC guidelines to ensure consistent application of the electronic communications policy on all TSTC campuses.

Further, the rules and procedures of this SOS shall ensure compliance with and the security of protected data required by the Family Educational Rights Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Texas Administrative Code, Title 1, Chapter 202, Subchapter C.

IV. DEFINITIONS

Information Resources (IR): 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 that include, but are not limited to, mainframes, servers, personal computers, notebook computers, handheld 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, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information on those resources.

V. DELEGATION OF AUTHORITY

The Chancellor has the authority to manage all aspects of the College’s operations related to information technology resources and delegates to the appropriate Vice Chancellor, or his/her designee, the responsibility to deploy resources, processes, and procedures to ensure compliance with this SOS and any applicable federal, state, and/or local regulations. Additionally, the designated Vice Chancellor has responsibility for all statewide procedures and governance documents related to information technology resources.

VI. PERFORMANCE STANDARDS

1. The designated Vice Chancellor, or his/her designee, tracks and measures the effectiveness of security controls for information resources owned or operated by TSTC.

2. The College’s policies and procedures related to information resources comply with federal privacy objectives under FERPA and HIPAA, as well as state regulations related to information security.

APPENDIX

VII. RELATED STATEWIDE STANDARDS. LEGAL CITATIONS, OR SUPPORTING DOCUMENT

Family Educational Rights Privacy Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Texas Administrative Code, Title 1, Chapter 202, Subchapter C
GA 5.1.1 Password Use and Management for Information Resources
GA 5.1.2 Management of Outsourced Information Services and Maintenance
GA 5.1.3 Information Technology User Account Management
GA 5.1.4 Acceptable Use of Information Technology Resources
GA 5.1.5 Managing Changes in Information Resources
GA 5.1.6 Data Classification and Handling Standard
GA 5.1.7 Information Technology Server Management
GA 5.1.8 Information Security Awareness and Training
GA 1.19 Disaster Recovery and Business Continuity Plan

VIII. OPERATING REQUIREMENTS:

The development and implementation of TSTC's guidelines and procedures required by this SOS shall be governed by specific procedural rules established by the designated Vice Chancellor, or his/her designee, and shall be documented in the College's body of SOS documents related to information technology resources, to include all forms of electronic communication.

Specifically, the full spectrum of the College's guidelines and procedures related to information technology resources must stipulate:

1. That individuals be accountable for their actions relating to information resources;
2. That information resources be used only for intended purposes as defined by TSTC and applicable laws;
3. That risks to information resources be managed;
4. That the integrity of data, its source, its destination, and the processes applied to it be assured;
5. That changes to data be made only in an authorized manner; and
6. That information resources be available when needed.

Additionally, the College's guidelines and procedures must ensure the continuity of information resources supporting critical TSTC operations in the event of a disaster or business disruption per GA 1.19 Disaster Recovery and Business Continuity Plan.