TEXAS STATE TECHNICAL COLLEGE

STATEWIDE OPERATING STANDARD

No. GA 5.1.2	**Page 1 of 5**	**Effective Date: 01/04/2019**
DIVISION:	**General Administration**	
SUBJECT:	**Management of Outsourced Information Services and Maintenance**	
AUTHORITY:	**Statewide Operating Standard GA 5.1**	
PROPOSED BY:	**Shelli Scherwitz**	
TITLE:	**Executive Vice President of Information Technology**	**Date: 01/04/2019**
RECOMMENDED BY:	**Rick Herrera**	
TITLE:	**Vice Chancellor/Chief Technology Officer**	**Date: 01/04/2019**
APPROVED BY:	**Mike Reeser**	
TITLE:	**Chancellor**	**Date: 01/04/2019**

STATUS: Approved by Leadership Team 01/04/2019

HISTORICAL STATUS: Approved by Chancellor 8/31/15
Revised 05/2015
Reviewed and Approved by Mini LA 6/10/14
Revised 6/2014
Approved by MC 4/11/13
Proposed 4/2013
Revised 6/2014
Reviewed 5/2015

I. STATEWIDE STANDARD

EXECUTIVE ORDER: By order of the Chancellor, Texas State Technical College (TSTC) shall establish standing orders as necessary to implement policy and procedures to secure the College's information technology resources, especially when those resources must be accessed by external vendors and/or contractors.

II. PERTINENT INFORMATION

Vendors play an important role in the support of computer hardware and software used at TSTC. In order to access the services of these qualified professionals, TSTC may allow vendors, from on-site and/or remote locations, to view, copy, modify data and view audit logs, correct software and operating systems problems, monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems, and reset alarm thresholds.

As access by outside vendors could pose a risk to TSTC and result in the loss of revenue, liability issues, loss of trust, and/or embarrassment, TSTC must set limits and controls on what can be remotely seen, copied, modified, and controlled by vendors in order to minimize the potential risk.

III. GENERAL GUIDELINES

This Statewide Operating Standard (SOS) regarding the management and maintenance of outsourced information services shall establish rules and requirements to allow TSTC vendors and contractors safe and secure access to TSTC information resources. Further, the rules and requirements 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

Contractor: An individual, association, corporation, or other business entity that undertakes a contract with TSTC to perform a service or to provide a product, or both.

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 Web sites, 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.

Office of Information Technology (OIT): The name of the College's department responsible for computers, networking, and data management.

Password: A string of characters that serves as authentication of a person's identity and that is used to grant or deny access to private or shared TSTC information

resources and/or data.

Vendor: An individual, association, corporation, or other business entity that exchanges goods or services for money.

V. DELEGATION OF AUTHORITY

The Chancellor has the authority to manage all aspects of the College's operations related to information resources and delegates to the appropriate Vice Chancellor, or his/her designee, the responsibility to deploy resources, processes, and procedures to manage information services and to ensure compliance with this SOS and any applicable federal and state regulations.

VI. PERFORMANCE STANDARDS

1. OIT personnel routinely verifies compliance with this SOS through various methods that include, but are not limited to, periodic document review, monitoring, business tool reports, internal and external audits, and feedback to the Vice Chancellor or to his/her designee.

2. **S**ecurity incidents are immediately reported directly to the appropriate TSTC technical point of contact.

3. OIT verifies that vendors have timely surrendered all TSTC identification badges, access cards, equipment, and supplies at the end of their contractual agreements.

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, Chapter 202, Subchapter C
GA 5.1 Password Use and Management for Information Resources

VII. OPERATING REQUIREMENTS:

TSTC, through its OIT personnel, must establish policies and procedures that set limits and controls on what TSTC information can be seen, copied, modified, and controlled by vendors. TSTC policies and procedures must focus on reducing, if not eliminating, potential risk to the College.

1. Vendors must comply with all applicable state and federal laws (HIPAA, FERPA, etc.), TSTC policies, practice standards and agreements. These include, but are not limited to:
   a. Safety policies;
   b. Privacy policies;
   c. Auditing policies; and
   d. The College's SOS documents related to information technology

2. Vendor agreements and contracts must specify or provide for the following, as applicable:
   a. The specific TSTC information accessible to the vendor;
   b. The vendor's policies and/or procedures to be implemented to protect the TSTC information;
   c. Approved methods for the return, destruction or disposal of TSTC information in the vendor's possession at the end of the contract; and
   d. Assurance that the vendor use TSTC information and its information resources only for the purposes set forth within the business agreement.

Vendor access standard(s) shall include, but not be limited to, the following:

1. Any TSTC information acquired by the vendor in the course of the contract shall not be used for the vendor's own purposes or be divulged to others.

2. Independent assurance of controls shall be instituted where applicable. Vendor assurance may be waived if the vendor does not have or cannot reach regulatory protected data and/or proprietary information.

3. TSTC shall provide a technical point of contact for the vendor for both on-site

and remote access. Vendor personnel must report all security incidents directly to the appropriate TSTC technical point of contact. The technical point of contact shall be defined on a system-by-system basis as the need arises.

4. Work hours and duties shall be defined in the contract. Work performed outside of the defined parameters must be approved in writing by the appropriate TSTC technical point of contact.

5. Vendor access must be uniquely identifiable and password management must comply with the Colleges' SOS GA 5.1 Password Use and Management for Information Resources.

6. Upon termination of the contract or at the request of TSTC, the vendor must return or destroy all TSTC information and provide written certification of that return or destruction within an agreed time frame.

7. Upon termination of the contract or at the request of TSTC, the vendor must immediately surrender all TSTC identification badges, access cards, equipment, and supplies unless authorized in writing to do otherwise by the appropriate TSTC technical point of contact.

8. Only the senior executive in charge of information technology shall be able to approve logical and/or physical access to any TSTC information resource.

9. Vendor access shall be reviewed at least annually by the OIT and compared to contract specifications.

10. Vendor access may be granted in emergency situations as approved by the senior executive in charge of information technology or the appropriate OIT Executive Director for the functional area impacted.

11. The senior executive in charge of information technology or appropriate OIT personnel for the functional area impacted may discontinue vendor access at any time if a significant real or perceived threat is discovered.