TEXAS STATE TECHNICAL COLLEGE
STATEWIDE OPERATING STANDARD

No. GA 5.1.1	**Page 1 of 5**	**Effective Date: 01/04/2019**
DIVISION:	**General Administration**	
SUBJECT:	**Password Use and Management for Information Resources**	
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: Approve by Leadership Team 01/04/2019

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

II. PERTINENT INFORMATION

User authentication is a means to control access to information resources. Controlling access is necessary for any information resource, because access by a non-authorized entity can result in loss of information confidentiality, integrity, and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to TSTC.

III. GENERAL GUIDELINES

This Statewide Operating Standard (SOS) regarding password use and management of information resources shall establish the rules for the creation, distribution, safeguarding, and termination of TSTC user authentication mechanisms. 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: 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.

Information Security Officer (ISO): The College’s designated employee in charge of information security for the entire institution.

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.

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 the responsibility to deploy resources, processes, and procedures to ensure compliance with this policy and any applicable federal and state regulations. Additionally, the designated Vice Chancellor has responsibility for all statewide procedures and governance documents related to information resources.

VI. PERFORMANCE STANDARDS

1. OIT personnel routinely verifies compliance with this SOS through various

methods that include, but are not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the ISO or to his/her designee.

2. All user passwords for TSTC-owned information resources are constructed with at least eight (8) characters and include a combination of letters and numbers.

3. Security tokens are accounted for and returned on demand or upon termination of the user's relationship with TSTC.

APPENDIX

VII. 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

VIII. OPERATING REQUIREMENTS:

1. All passwords must be constructed and implemented according to the specific requirements set forth by the individual application manager(s). If no guidance exists, the password must be constructed using at least eight (8) characters and must include a combination of letters and numbers.

2. User passwords stored in TSTC information resources must be encrypted or protected from disclosure except to the user.

3. User account passwords must not be divulged to anyone. TSTC OIT and contractors shall not ask for or receive access to user account passwords.

4. Security tokens (i.e. Smartcards) must be returned on demand or upon termination of the user’s relationship with TSTC.

5. If the security of a password is in doubt, the password must be changed immediately.

6. Anyone given access to TSTC-owned information resources shall not circumvent password entry with auto logon, application remembering, embedded scripts, hardcoded passwords in client software, or web browser credential remembering features. Exceptions may be made for specific applications (like automated backup) with the approval of the ISO. In order for an exception to be approved, there must be a procedure to change the password.

7. Computing devices must not be left unattended without enabling a password-protected screensaver. The user may meet this requirement by logging off of the device.

8. The OIT Help Desk change procedures for passwords must require the following:
   a. Help Desk personnel must authenticate the user before changing password; and
   b. The user must change password at first login.

9. In the event that passwords are openly discovered, TSTC personnel must take the following steps:
   a. Take control of the passwords and protect them;

b. Report the discovery to the OIT Help Desk; and
c. Transfer the passwords to an authorized person as directed by the ISO.

10. Any legacy or third-party application in use prior to the acceptance of this SOS that cannot comply with this standard shall be subject to a life cycle review. Based on that review, recommendations shall be made to secure the application with reasonable means. The ISO shall document the resulting action.