TEXAS STATE TECHNICAL COLLEGE
STATEWIDE OPERATING STANDARD

No. GA 5.1.3	**Page 1 of 5**	**Effective Date: 01/22/2019**
DIVISION:	**General Administration**	
SUBJECT:	**Information Technology User Account Management**	
AUTHORITY:	**Statewide Operating Standard GA 5.1**	
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 Leadership Team 01/22/2019

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

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 in regards to user accounts granting access to TSTC information and resources.

II. PERTINENT INFORMATION

User accounts are the means used to grant access to TSTC 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) shall establish the rules and requirements for the creation, monitoring, control, and removal of user accounts. These rules and requirements shall apply equally to all individuals with authorized access to any of the College's information resources. Approval for creating or modifying user accounts and their access rights shall be restricted to the Data Owner of a respective information resource.

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

Application Administrator: Person or persons responsible for the effective operation and maintenance of account management, including implementation of standard procedures and controls used to manage the information resources.

Application Manager: Person with overall responsibility for the day-to-day operations of an information resources, including the approval of new user accounts and applicable access rights for a user of a specific information resource.

Data Owner: Person responsible for approving user accounts and granting access rights to a specific data set within an information resource by its Application Manager. There may be multiple Data Owners within an information resource, but only one Data Owner for a defined data set.

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.

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

V. DELEGATION OF AUTHORITY

The Chancellor has the authority to manage all aspects of the College's operations in regards to information resources and delegates to the appropriate Vice Chancellor the responsibility to deploy resources, processes, and procedures to ensure compliance with this Statewide Operating Standard (SOS) and any applicable federal, state and/or local regulations.

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 Vice Chancellor or to his/her designee.

2. Application Manager publishes security requirements for information resource user accounts and advises users of requirements.

3. OIT suspends user accounts that do not have proper authorization until proper authorization is obtained.

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
GA 5.1.1 Password Use and Management for Information Resources

VIII. OPERATING REQUIREMENTS:

Specific Information Regarding Assigned Duties:

1. Application Administrators shall perform all changes to user accounts and access rights based on the *User Account Request and Approval Process* noted below.
    a. Administrators must have a documented process to modify a user account to accommodate situations such as name changes, account changes, and permission changes. The Application Manager shall review existing accounts for validity as reported by the Application Administrator.
    b. Administrators shall be subject to independent audit reviews and must provide a list of accounts for the information resources they administer.
    c. As requested by an authorized member of TSTC management, administrators must cooperate with all parties in the investigation of security incidents.
2. The Application Manager shall identify any applicable forms and rules required for users. The Application Manager shall also decide if a user's specific information resource has expanded data sets that require delegation of account creation and applicable access rights to a Data Owner. There may be multiple people involved in the management of an information resource, but there shall be only one Application Manager responsible for a specific information resource.
3. There may be multiple Data Owners within an information resource, but there shall be only one Data Owner for a defined data set. The Application Manager shall will be responsible for managing the use of Data Owners, applicable forms, and rules to be followed.

User Account Request and Approval Process:

1. Procedures for user account request, approval, creation, modification, and removal shall be approved and published for that application by the Application Manager.
2. The Application Manager shall advise users requesting access to any information resources for all applicable security requirements.
3. The user and his/her supervisor shall submit the user account request to the Application Manager or Data Owner for approval. Any additional forms or agreements shall be provided to, and signed by, the user and stored accordingly by the Application Manager.
4. The Application Manager or Data Owner may reject or modify the user account request.
5. Approved changes to user accounts and access rights shall be forwarded to

the Application Administrator for processing.

6. In the event of a separation from employment or an extenuating circumstance, a request to terminate user account access may be submitted by an authorized member of TSTC management and approved by the Human Resources Department without informing the user and/or Application Manager.

User Account Management:

1. All user accounts must be uniquely identifiable with the user's assigned username. All passwords for user accounts shall adhere to requirements stipulated in the College's SOS GA 5.1.1 Password Use and Management for Information Resources**.**
2. User accounts for mission critical information resources must be reviewed, at a minimum, on an annual basis. User accounts for non-mission critical information resources must be reviewed, at a minimum, on a bi-annual basis.
3. OIT shall conduct periodic reviews of user accounts to mission critical Information Resources. Any user account that does not have proper authorization shall be suspended until such authorization can be obtained.