TEXAS STATE TECHNICAL COLLEGE

STATEWIDE OPERATING STANDARD

No. GA 5.1.3	**Page 1 of 3**	**Effective Date: 08/31/15**
DIVISION:	**General Administration**	
SUBJECT:	**Information Technology User Account Management**	
AUTHORITY:	**Statewide Operating Standard GA 5.1**	
PROPOSED BY:	***Original Signed by Rick Herrera***	
TITLE:	**Vice Chancellor & Chief Technology Officer**	**Date: 08/31/15**
RECOMMENDED BY:	***Original Signed by Rick Herrera***	
TITLE:	**Vice Chancellor & Chief Technology Officer**	**Date: 08/31/15**
APPROVED BY:	***Original Signed by Mike Reeser***	
TITLE:	**Chancellor**	**Date: 08/31/15**

STATUS: Approved by the Chancellor 08/31/15

HISTORICAL STATUS: 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

Executive Order

INTRODUCTION:

Computer accounts are the means used to grant access to TSTC Information Resources. Approval for creating or modifying computer accounts and their access rights is restricted to the System or Data owner for a respective information resource.

PURPOSE:

The purpose of the TSTC Account Management Standard is to establish the rules for the creation, monitoring, control and removal of user accounts.

AUDIENCE:

The TSTC Account Management Standard applies equally to all individuals with authorized access to any TSTC Information Resources.

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 Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but 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 and 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.

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 Resource.

Application Manager: Person with overall responsibility for the day-to-day operations of an Information System. This responsibility includes the approval of new accounts and applicable access rights for a user of a specific Information Resource. This individual will identify any applicable forms and rules that will need to be adhered to by the user. The Application Manager will also decide if their specific Information Resource has expanded data sets that will require the need to delegate 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 will only be one person assigned Application Manager responsibilities for a specific Information Resource.

Data Owner: Person assigned the responsibility of 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 there will be only one Data Owner for a defined data set. The Application Manager will be responsible for managing the use of Data Owners, applicable forms and rules to be followed.

ACCOUNT MANAGEMENT STANDARD:

Account Approval Process:

1. The Application Manager will advise users requesting access of any applicable security requirements.
2. Procedures for account creation, modification and removal will be will be defined and published for that application. The Application Manager for each application will approve the related procedures.
3. The request is submitted by the User and their Supervisor (if applicable) and forwarded to the Application Manager or Data Owner for approval. Any additional forms or agreements will be provided to and signed by the User and stored accordingly by the Application Manager.
4. Application Manager or Data owner may reject or modify the request as applicable.
5. Approved changes to accounts and access rights are forwarded to the Application Administrator for processing.
6. In the event of a separation of employment or extenuating circumstance, a request to terminate account access may be submitted by appropriate management and approved by the HR/HOD department without informing the User and/or Application Manager.

Account Management:

1. All accounts must be uniquely identifiable using the user's assigned username. All passwords for accounts will adhere to the TSTC Password Standard.
2. Accounts to mission critical information resources must be reviewed annually at a minimum. Accounts to non-mission critical information resources must be reviewed bi-annually at a minimum.
3. OIT will conduct periodic reviews of accounts to mission critical information resources. Any account that does not have proper authorization will be suspended until such authorization can be obtained.

Application Administrators:

1. Are responsible for performing changes to User accounts and access rights based on the Account Approval Process noted above.
2. Must have a documented process to modify a user account to accommodate situations such as name changes, account changes and permission changes. It is the responsibility of the Application Manager to review existing accounts for validity as reported by the Application Administrator.
3. Are subject to independent audit review and must provide a list of accounts for the systems they administer. Also, as requested by authorized TSTC management, they must cooperate with all parties in the investigating of security incidents.

DISCIPLINARY ACTIONS:

Non-compliance with established standards and rules and procedures will subject an employee to a range of corrective actions pursuant to SOS HR 2.4.1 Employee Corrective Action.