TEXAS STATE TECHNICAL COLLEGE
STATEWIDE OPERATING STANDARD

No. GA 5.1. 5	**Page 1 of 4**	**Effective Date: 8/31/15**
DIVISION:	**General Administration**	
SUBJECT:	**Managing Changes in Information Resources**	
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
Reviewed 6/2014
Approved by MC 1/15/14
Proposed 12/2013

EXECUTIVE ORDER

INTRODUCTION

The Information Resources infrastructure at TSTC is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources data and infrastructure grows, the need for a strong change management process is essential.

PURPOSE

The purpose of the Change Management Standard is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

AUDIENCE

The TSTC Change Management Standard applies to all individuals who install, operate or maintain TSTC information resources.

DEFINITIONS

Information Resources (IR): any and all 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. Additionally, it is 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.

System Owner: 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 System Owner 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 System Owner 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 System Owner. There may be multiple Data Owners within an Information Resource, but there will be only one Data Owner for a defined data set. The System Owner will be responsible for managing the use of Data Owners, applicable forms and rules to be followed.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification.

Change:

- any implementation of new functionality
- any repair that will result in a change in functionality
- any repair of existing functionality
- any removal or modification of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.

CHANGE MANAGEMENT STANDARD

- Changes to data made by the end-user are presumed authorized based on access management practices.
- Any change that returns the system to its prior operational state will not require approval prior to change
- Changes to data made by OIT personnel on behalf of system and/or data owner(s) must have documented permission from the system and/or data owner(s).
- A written change request must be submitted for all material changes, both scheduled and unscheduled.
- Material changes that may affect Federal or State reporting must be cleared by system and data owner(s).
- Appropriate audit trails shall be maintained to provide accountability for updates to data, hardware and software and for all changes to automated security or access rules where applicable. If an information resource cannot support automated audit trails manual documentation will exist in order to track and/or audit changes. The risk shall be disclosed to appropriate management.
- All material security-related information resource changes shall be approved by the system owner and data owner(s). The risk of the change will be disclosed and approval shall occur prior to implementation.
- Planning for the implementation of an approved change will include back-out procedures should implementation of the change be cancelled.
- Planning for the implementation of an approved change will include post-change testing to validate the change is functioning properly
- Changes that require the service to be brought down for any period of time should be scheduled for outside of normal business hours where applicable and approved by the respective system and data owner(s).
- When a test environment is available, all changes will be validated in the test environment before implementation
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

    - Date of submission and date of change
    - Owner and custodian contact information
    - Nature of the change
    - Indication of success or failure
    - The name of the approver

- The name of the person making the change

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.