TEXAS STATE TECHNICAL COLLEGE SYSTEM

SYSTEM OPERATING STANDARD

No. GA 5.1	**Page 1 of 2**	**Effective Date: 2/7/13**
DIVISION:	**General Administration**	
SUBJECT:	**Information Technology**	
AUTHORITY:	**Minute Order #21-13**	
PROPOSED BY:	***Original Signed by Rick Herrera***	
TITLE:	**Vice Chancellor and Chief Technology Officer**	**Date: 2/7/13**
RECOMMENDED BY:	***Original Signed by Mike Reeser***	
TITLE:	**Management Council**	**Date: 2/7/13**
APPROVED BY:	***Original Signed by Mike Reeser***	
TITLE:	**Chancellor**	**Date: 2/7/13**

STATUS: Approved by BOR 2/7/13

HISTORICAL STATUS: Original Proposed 2/7/13
Formerly Titled: Information Technology Resource Management

POLICY

It is the policy of Texas State Technical College (TSTC) that information technology (IT) is effectively and efficiently governed in a manner that supports the goals and objectives of the College System; considers applicable regulations, guidelines, standards, and best practices; and results in the protection, availability and security of technology assets and data.

PERTINENT INFORMATION

Information Resources owned and operated by TSTC shall be available and protected commensurate with the value of the resource. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to state information resources shall be appropriately managed.

All individuals are accountable for their actions relating to information resources.

Information resources shall be used only for intended purposes as defined by TSTC and consistent with applicable laws.

Risks to information resources shall be managed.

The integrity of data, its source, its destination, and processes applied to it shall be assured.

Changes to data shall be made only in an authorized manner.

Information resources shall be available when needed.

Continuity of information resources supporting critical College operations shall be ensured in the event of a disaster or business disruption.

Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.

DELEGATION OF AUTHORITY

Deployment of resources that are consistent with this policy, as well as the IT Operating Standards (ITOS) and IT Application Governance Documents will be the responsibility of the Chief Technology Officer acting on behalf of the Chancellor.

OPERATING REQUIREMENTS

This policy will be implemented by establishing general ITOS governing the components of the policy. Specific procedural rules by IT system will be established in IT Application Governance Documents.

All ITOS will be reviewed by an IT Steering Committee. The IT Steering Committee will be comprised of a cross-functional group representative of all campuses. The committee's membership will be approved by Management Council. This committee will be responsible for creating the final draft of all ITOS.

Management Council will be the final approving authority of all ITOS. Implementation of the ITOS may be done through an Executive Order of the Chancellor.

PERFORMANCE STANDARDS

Measurements will be defined and tracked to ensure effective and efficient use of resources as they pertain to achieving business objectives.