TEXAS STATE TECHNICAL COLLEGE

STATEWIDE OPERATING STANDARD

No. GA 5.1.7	**Page 1 of 4**	**Effective Date: 02/19/16**
DIVISION:	**General Administration**	
SUBJECT:	**Information Technology Server Management**	
AUTHORITY:	**Statewide Operating Standard GA 5.1**	
PROPOSED BY:	**Rick Herrera**	
TITLE:	**Vice Chancellor & Chief Technology Officer**	**Date: 02/19/16**
RECOMMENDED BY:	***Original Signed by Rick Herrera***	
TITLE:	**Vice Chancellor & Chief Technology Officer**	**Date: 02/19/16**
APPROVED BY:	***Original Signed by Mike Reeser***	
TITLE:	**Chancellor**	**Date: 02/19/16**

STATUS: Approved by VCs 02/19/16

HISTORICAL STATUS: New/Proposed 01/2016

Executive Order

INTRODUCTION:

Servers are utilized to deliver critical components of instruction, research, faculty development, student services, and administration in pursuit of the TSTC mission. The following are College-wide server management practices that define roles, responsibilities, procedures and controls encourage consistent, secure, and responsible delivery of services.

PURPOSE:

This operating standard establishes the framework under which College servers are managed to promote availability, secure assets, and mitigate vulnerabilities.

SCOPE:

This operating standard applies to all TSTC servers, whether administered remotely, centrally or departmentally, and regardless of where they reside.

DEFINITIONS:

Server Owner: The server owner is responsible for the management, operation, and security of the server. Server administration functions may be designated; however, the server owner retains ultimate responsibility for the server hardware and OS. These responsibilities may include server management compliance in fiscal planning, business/academic continuity planning, and personnel resource planning. The owner is also responsible for ensuring proper training for server administrators.

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.

Server Administrator: An individual designated by the server owner as principally responsible for performing server management functions, including but not limited to hardware installation, server configuration, security, monitoring, maintenance and registration.

Application Administrator: An authorized person responsible for the administration of one or more applications. An application administrator's responsibilities typically include application configuration, account management, installation of software upgrades, and user support.

Instructional Server: A server that is used expressly for the purpose technology related instruction. These servers are physically and logically separated from the TSTC operational networks.

SERVER MANAGEMENT STANDARD:

Any server that is connected to the College's network must comply with this standard, related standards, established procedures, and applicable regulatory requirements.

Documentation and Usage

- All uses of servers must comply with TSTC Acceptable Use Standard (GA 5.1.4)
- All changes to servers and applications residing on servers will comply with TSTC Change Management Standard (GA 5.1.5)
- Operational procedures established for day-to-day server operations must be documented and available for periodic review.
- All servers and applications residing on servers must be registered with Office of Information Technology (OIT).
- OIT will maintain a listing of all servers and related applications including the designated application administrators, server administrators, and owners.
- OIT must be notified in advance when the purpose, location, management, administrator, and/or configuration of the server changes.

Server Ownership

- All servers must have an owner and administrator(s) assigned.
- The Chief Technology Officer (CTO) is considered owner of all servers hosting enterprise applications.
- No server will be deployed on the TSTC operational network without the approval of the CTO and/or Senior Executive Director of Infrastructure.

Server Procurement

- Prior to the purchase of any server, the server owner should contact OIT to evaluate the capabilities required to maintain server compliance and review alternative solutions where applicable.
- The purchase of a server in support of a new installation must be included in an approved project brief.
- The System Owner(s) affected by the server being replaced will approved the implementation timeline of a replacement server.

Environmental and Facility Controls

- Servers must reside in an OIT approved secure area.
- Servers will be physically and environmentally protected to include, but not limited to:
    - Restricted physical access
    - Climate control
    - Uninterrupted power supply
    - Fire suppression device

Server Maintenance and Security

- Logical administrative access will only be allowed through secure protocols and authentication methods.
- All server operating systems and applications on those systems will be patched per the vendor's specifications where applicable. Exceptions must be documented.
- Vulnerabilities will be communicated to the server owner and server administrator for resolution. The Server owner must respond with an acknowledgement within 3 days. Servers with unresolved vulnerabilities are subject to disconnect after 3 or more days.
- Servers that pose an immediate threat to network operations, performance, or security may be immediately disconnected or quarantined without notification until the threat is removed.

Backup and Recovery

- All information and applications residing on servers shall be backed up as appropriate based on criticality of the server, application, and/or data present on server.
- Server administrators will ensure servers and applications can be recovered in the event of catastrophic failure.

EXEMPTIONS:

There may be situations where certain servers may qualify for an exemption from this standard. In order for a server to qualify for an exemption, the server owner must apply for the exemption using the Server Request Form located in the Portal.

The Exec Director of Infrastructure and/or Chief Technology Officer must approve exemptions. In the event the exemption is not granted, the Server Owner may request an appeal through their respective Vice Chancellor.

The following are key components for a server to be exempt from any of the above stated standards:

- Is logically separate from the TSTC operational network.
- Does not contain, process, or output any data that is regarded as regulatory protected.
- Maintenance and/or administration plan is defined and shared with the OIT department.

DISCIPLINARY ACTIONS:

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