TEXAS STATE TECHNICAL COLLEGE
STATEWIDE OPERATING STANDARD

No: GA 5.1.4	**Page 1 of 5**	**Effective Date: 5/26/2017**
DIVISION:	General Administration	
SUBJECT:	Acceptable Use of Information Technology Resources	
AUTHORITY:	Statewide Operating Standard GA 5.1	
PROPOSED BY:	Rick Herrera	
TITLE:	Vice Chancellor/Chief Technology Officer	**Date: 5/26/2017**
RECOMMENDED BY:	Rick Herrera	
TITLE:	Vice Chancellor/Chief Technology Officer	**Date: 5/26/2017**
APPROVED BY:	Original Signed by Mike Reeser	
TITLE:	Chancellor	**Date: 5/26/2017**

STATUS: Approved by Leadership Team 5/26/2017

HISTORICAL STATUS: Approved by the Chancellor 08/31/15
Revised 05/2015
Reviewed and Approved by Mini LA 6/10/14
Reviewed 6/2014
Approved by MC 4/11/13
Proposed 4/2013

EXECUTIVE ORDER

INTRODUCTION

Under the provisions of the Information Resources Management Act, Information Resources are strategic assets of TSTC that must be managed as valuable resources. This standard is established to achieve the following:

1. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
2. To establish prudent and acceptable practices regarding the use of information resources.
3. To educate individuals who may use information resources with respect to their responsibilities associated with such use.

PURPOSE

The purpose of the TSTC Acceptable Use Standard is to establish the rules for use of TSTC owned information resources.

AUDIENCE

The TSTC Acceptable Use Standard applies 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.

User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules

Personal Devices: Any employee owned electronic devices connecting to TSTC resources. This includes, but is not limited to, smartphones, laptops, tablets, and desktops.

Portable Media: Any portable device used for the purpose of storing data. This includes, but is not limited to, flash drives and portable hard drives.

Cloud Services: Any service made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from TSTC's on-premises servers.

TSTC Data: All data or information held on behalf of TSTC, created as a result and/or in support of TSTC business, or residing on TSTC information resources, including paper records.
Sensitive Personal Information (SPI): An individual's name in combination with sensitive data elements such as social security number, health conditions, or credit card numbers. For additional detail see SOS GA 5.1.6 Data Classification and Handling Standard

FERPA Protected Information: Any other student data elements that TSTC has not determined to be directory information as per SOS GA 1.5.2 Student Records. For additional detail see SOS GA 5.1.6 Data Classification and Handling Standard

Open Records Requests: Information resources processing TSTC data become subject to open records requests as per Texas Government Code Chapter 552.002. More information can be located in SOS GA 1.5.3 Texas Public Information Act.

ACCEPTABLE USE STANDARD

All users of information resources owned by TSTC or personal devices connected to the TSTC network are required to adhere to the following:

- Users should not attempt to access any data or programs contained on TSTC information resources for which they do not have authorization;
- users must not share their TSTC account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), employee ID cards, or similar information or devices used for identification and authorization purposes;
- users must not make unauthorized copies of copyrighted software;
- users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of TSTC Information Resources; deprive an authorized TSTC user access to a TSTC resource; obtain extra resources beyond those allocated; circumvent TSTC computer security measures;
- users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, TSTC users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on TSTC Information Resources (other than in the course of security testing and troubleshooting by authorized OIT personnel);
- users must not use TSTC Information Resources for personal gain;
- users must not intentionally access, create, store or transmit material which TSTC may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the TSTC official processes for dealing with academic ethical issues); and
- users must not otherwise engage in acts against the aims and purposes of TSTC as specified in its governing documents or in rules, regulations and procedures.

Incidental Use

As a convenience to the TSTC user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to TSTC approved users; it does not extend to family members or other acquaintances;
- incidental use must not result in material direct costs to TSTC;
- incidental use must not interfere with the normal performance of an employee's work duties;
- no files or documents may be sent or received that may cause legal action against, or embarrassment to TSTC; and
- storage of personal email messages, voice messages, files and documents within TSTC's Information Resources must be nominal.

All messages, files and documents – including personal messages, files and documents – located on TSTC Information Resources are owned by TSTC, may be subject to open records requests, and may be accessed in accordance with this standard.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of TSTC are not private and may be accessed by TSTC with approval of Executive Management or legal counsel at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. TSTC information resources are subject to activity logging.

Insider Threats

All users of information resources are expected to use resources in an ethical manner to further the mission of TSTC. Upon the discovery of an employee, coworker, or affiliate of TSTC exceeding or abusing authorized access to information resources, the user should notify both the TSTC Helpdesk and their supervisor to ensure that the incident is reviewed appropriately. To anonymously report insider threats, the employees can utilize the TSTC Hotline - EthicsPoint linked at http://www.tstc.edu/footer/fraudwasteabuse.

Personal Devices

As a convenience to the TSTC user community, TSTC allows the use of personal devices for common tasks such as checking email. The following restrictions apply to personal devices used to access TSTC resources:

- Personal devices must be used in accordance with applicable rules, regulations, policies, and standards while connected to the TSTC network;
- personal devices connecting to TSTC resources should have antivirus software installed and updated to the latest version available;
- personal devices should be updated to the latest version of their respective operating system as the device vendor permits;
- personal devices processing TSTC data may be subject to open records requests;
- personal devices should utilize a password, pattern or pin code to access the device. This password, pattern or pin code must not be shared with other users;
- users must not store SPI data or FERPA protected data on personal devices;
- personal devices violating applicable rules, regulations, policies, and standards, or which present a risk to TSTC resources will be subject to a temporary or permanent block;
- upon separation or termination of an employee from TSTC, all TSTC data must be wiped from all personal devices;
- personal devices may not utilize peer-to-peer file sharing services (e.g. BitTorrent) while connected to the TSTC network; and
- all security incidents or violations on personal devices, such as malware, virus, or a lost or stolen device, must be reported to a supervisor and the TSTC Helpdesk.

Portable Media

TSTC allows the use of portable media to enable the collaboration between local users. The following restrictions apply to portable media containing TSTC data:

- Users must not store unencrypted SPI data or FERPA protected data on portable media;
- upon the disposal of a portable media device, the TSTC Help Desk must be contacted for proper destruction to ensure the protection of TSTC data;
- upon separation or termination of an employee from TSTC, all portable media containing TSTC data will be returned to TSTC; and
- all security incidents or violations relating to portable media, such as a lost or stolen flash drive, must be reported to a supervisor and the TSTC Help Desk.

Cloud Services

TSTC provides a number of cloud services to employees, such as Google products. The use of cloud services has dramatically increased over the years and certain limitations are in place to protect TSTC data. The following restrictions apply to the use of cloud services:

- All cloud services must be reviewed and approved by The Office of Information Technology prior to using cloud services to ensure the protection of TSTC data. A pre-approved list of services will be made available;
- addons or plugins connecting to cloud services must be approved by The Office of Information Technology. Unapproved cloud service addons or plugins may be blocked;
- users must not store unencrypted SPI data or FERPA protected data on cloud services. Exceptions may be issued upon a contract, security review and approval of the cloud service by the Chief Technology Officer;
- all cloud services processing TSTC data will be subject to open records requests;
- users must use approved cloud services in accordance with applicable rules, regulations, policies, and standards; and
- cloud services that pose a threat to TSTC resources or TSTC data may be subject to a temporary or permanent block.

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.