TEXAS STATE TECHNICAL COLLEGE
STATEWIDE OPERATING STANDARD

No. GA 5.1.6	**Page 1 of 4**	**Effective Date: 8/31/15**
DIVISION:	**General Administration**	
SUBJECT:	**Data Classification and Handling Standard**	
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 06/2015
Reviewed and Approved by MC 09/24/14
Approved by Mini LA 09/12/14
Proposed 9/2014

EXECUTIVE ORDER

INTRODUCTION:
Data classification and handling provides a framework for classifying and securing data based on the associated risks, as well as for applying the appropriate levels of protection as required by State and/or federal law taking into consideration proprietary, ethical, operational, and privacy concerns. All Texas State Technical College (TSTC) data, whether electronic or printed, should be categorized with these criteria.

PURPOSE:
The purpose of the TSTC Data Classification and Handling Standard is to establish definitions and minimum criteria for data created, stored, transmitted, and used by TSTC and its authorized extensions.

AUDIENCE:

The TSTC Data Classification and Handling Standard apply to all TSTC owned data.

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, tablet 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.

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.

Sensitive Personal Information (SPI): An individual's first name or first initial and last name in combination of any one or more of the following items, if the name and the items are not encrypted.

- Social security number;
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Information that identifies an individual and relates to:
- The physical or mental health or condition of the individual;
- The provision of health care to the individual;
- Payment for the provision of health care to the individual.

Personally Identifiable Information (PII): Information that alone or in conjunction with other information identifies an individual, including an individual's:

- Name, date of birth, or government-issued identification number;
- Mother's maiden name;
- Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- Unique electronic identification number, address, or routing code; and
- Certain telecommunication access device as defined by regulation

FERPA Protected Information: Any information that TSTC has not determined to be directory information and must be consented to by the student prior to release. Examples include:

- Any SPI or PII data element
- Grades Point Average/Letter Grades
- Academic Standing
- Indication of Financial Aid Status
- Counseling records
- Academic Comments

General Information: Any information that is not related to SPI, PII, and/or FERPA or not otherwise protected by regulation(s) and/or publically available. This information will include most directory information. Examples include a person's:

- Name along with residential address and/or telephone numbers.
- Email address
- Age and Sex
- Title or Position

SPI DATA HANDLING STANDARD:

- All SPI data elements must be encrypted upon removal from source repository.
- All SPI must be purged as soon as reasonably possible if residing outside source repository.
- Only authorized individuals may have access to SPI.
- Appropriate audit trails will be established for information resources that contain SPI data.
- Access to SPI data will only be granted by the data owner or designee
- SPI data transmitted over public networks must be encrypted.
- Any agreements with third parties that involve SPI data must be assessed by OIT .
- Any employee that suspects SPI data has been compromised, lost, or otherwise disclosed without authorization must disclose the incident immediately to their supervisor, the Information Security Officer and Chief Technology Officer.

PII DATA HANDLING STANDARD:

- Any PII data element alone or in combination must have the approval of the data owner, application manager, or designee prior to being accessed from the source repository.
- Any record and/or document with more than 3 PII data elements must be encrypted prior being transmitted and/or stored on public networks.
- PII data stored outside the source repository must be purged as soon as reasonably possible.
- Any PII data processed and/or stored by a third-party application must have the approval of the data owner, application manager, or designee.
- Any agreements with third parties that involve PII data must be assessed by OIT.

- Any employee that suspects that PII data has been compromised, lost, or otherwise disclosed without authorization must disclose the incident immediately to their supervisor and the Information Security Officer or Chief Technology Officer.

FERPA PROTECTED DATA HANDLING STANDARD:

- All FERPA protected data element alone or in combination must have the approval of the data owner, application manager, or designee prior to being accessed from the source repository.
- Any FERPA protected data element that can be easily associated with the individual student must be encrypted prior to being transmitted and/or stored on public networks.
- FERPA protected data stored outside the source repository must be purged as soon as reasonably possible.
- Any FERPA protected data processed and/or stored by a third-party application must have the approval of the data owner, application manager, or designee.
- Any agreements with third parties that involve PII data must be assessed by OIT.
- Any employee that suspects that FERPA data has been compromised, lost, or otherwise disclosed without authorization must disclose the incident immediately to their supervisor and the Information Security Officer or Chief Technology Officer.

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.