SOUTH TEXAS COLLEGE

INFORMATION SECURITY OFFICE

Document Name:	**Data Classification Standard**
Document Number:	ISO.RA-2.S.2
Supersedes:	None
Approved by:	Victor M. Gonzalez, Chief Information Security Officer Alicia Gomez, Chief Information Officer
Effective date:	6/13/2017

1. OVERVIEW

Pursuant to Texas Administrative Code §202.74, institutions of higher education are responsible for defining all information classification categories except the confidential information category, which is defined in Subchapter A of § 202.74 as "information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act". A data classification standard is necessary to provide a framework for securing data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal.

2. PURPOSE

The purpose of this standard is to define the classification categories that will be used to classify data and information resources owned by the College. The classification will permit the College to protect these resources based on the impact of losing the confidentiality, availability or integrity of the data. The proper classification of the information resource will mandate the set of security controls that must exist to properly secure the information.

3. SCOPE

This standard applies to all centrally managed enterprise-level administrative data and to all user-developed data sets and systems that may access these data, regardless of the environment where the data reside (including mainframe systems, servers, personal computers, laptops, etc.). The standard applies regardless of the media on which data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

4. STANDARD

There are three classification categories that shall be used to classify information and information resources. These classifications will be based on the impact of losing the confidentiality, integrity, or availability of this information. This impact can be financial, reputational, legal, or to the safety of individuals.

Security Objectives	FIPS 199 Definition
Confidentiality	A loss of confidentiality is the unauthorized disclosure of information.
Integrity	A loss of integrity is the unauthorized modification or destruction of information.
Availability	A loss of availability is the disruption of access to or use of information or an information system.

Table 1: Information and Information Resource Security Objectives

4.1. Confidential Classification Category (High Impact)

This category shall be applied when the protection is required by law or there is a potential for an adverse impact to College operations and assets, or individuals.

4.2. Restricted Classification Category (Moderate Impact)

This category shall be applied on data or information resources not covered under High impact, but where there is still a responsibility to protect based on an individual's right to opt-out or information that needs to be restricted until requested through an official process.

4.3. Public Classification Category (Low Impact)

This category includes all information that is not covered under the High or Moderate classification. The protection of the information is at the discretion of the owner or custodian.

5. ROLES AND RESPONSIBILITIES

5.1. Data Owner

Data owners are senior College officials (or their designees) who have planning and policy-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management for the good of the entire College.

5.2. Data Custodian

The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees (usually the data stewards), and implementing and administering controls over the information.

5.3. Data Steward

Data stewards are College officials having direct operational-level responsibility for information management – usually department directors. Data stewards are responsible for data access and policy implementation issues.

5.4. Data User

Data users are individuals who need and use College data as part of their assigned duties or in fulfillment of assigned roles or functions within the College community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.

6. RELATED GUIDANCE

- ISO.RA-2.G.1: Data Classification Guidelines v1809
- NIST SP 800-60v1r1: Guide for Mapping Types of Information and Information Systems to Security Categories
- FIPS Pub 199

7. CHANGE HISTORY

Date	Name	Description
2/18/2017	Victor M. Gonzalez	Initial draft
4/05/2017	Victor M. Gonzalez	Received feedback from CIO
6/13/2017	Victor M. Gonzalez	Published
8/29/2017	Victor M. Gonzalez	Added security objectives table for clarification and added related guidance items
10/09/2018	Orlando J. Gomez	Updated related guidance – ISO.RA-2.G.1: Data Classification Guidelines v1809