Procedure III.3010.A.e, Data Security

Associated Policy
Policy III.3010.A, Information Resources

Related Policies
Policy VI.6000.B, Confidentiality of Student Records

1. Purpose

This Procedure describes these requirements and expected responsibilities for identifying, classifying, and applying the appropriate security controls to the College's data. The College's Information Resources are vital academic and administrative assets that require appropriate safeguards. Computer systems, networks, and data are vulnerable to ever-increasing cybersecurity threats. These threats have the potential to perpetrate financial fraud and compromise the Confidentiality, Integrity, and Availability of the information used to conduct its College Business. To combat these threats, Federal and State Laws require the College to take measures to protect Information Resources against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate.

2. Applicability

This Procedure applies to all Users of College Information Resources, in any form, and is intended to be broad enough to include all Users.

3. Laws, Regulations, and Standards

The College is required to comply with Federal and Texas State Laws and Regulations. In the 86th legislative session, the Texas Legislature enacted policy that requires the College to comply with state information security standards, including mandatory cybersecurity training for elected officials, employees, and contractors. Furthermore, in the 87th legislative session, the Texas Legislature enacted policy that requires the College to designate a Data Management Officer (DMO) to establish a data governance program to identify data assets, establish processes and Procedures to oversee the College's data assets, and implement practices and controls for managing and securing the College's data. The College is also required to comply with Federal Laws and Regulations that include but are not limited to, the Family Educational Rights and Privacy Act (FERPA), Gram-Leach-Bliley Act (GLBA), Personal Credit Information (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Children's Online Privacy Protection Act (COPPA).

4. Associated Program Controls

The following Program Controls associated with this Procedure are:

AT Awareness and Training Control Family

- AT-2 Awareness and Training | Literacy Training and Awareness
- AT-3 Awareness and Training | Role-Based Training

- AT-4 Awareness and Training | Training Records

CM Configuration Management Control Family

- CM-10 Configuration Management | Software Usage Restrictions
- CM-11 Configuration Management | User-Installed Software

RA Risk Assessment Control Family

- RA-2 Risk Assessment | Security Categorization (Sensitivity Levels)

Media Protection Control Family

- MP-6 Media Protection | Media Sanitization
- MP-6(1) Media Protection | Media Sanitization | Review, Approve, Track, Document, And Verify-2 | Security Categorization IR-6 Incident Reporting
- MP-2 Media Protection | Media Access
- MP-7 Media Protection | Media Use

SC System and Communication Protection

- SC-5 System and Communication Protection | Denial of Service Protection
- SC-7 System and Communication Protection | Boundary Protection
- SC-8 System and Communication Protection | Transmission Confidentiality and Integrity
- SC-12 System and Communication Protection | Cryptographic Key Establishment and Management
- SC-13 System and Communication Protection | Cryptographic Protection

SI System and Information Integrity Control Family

- SI-2 System and Information Integrity | Flaw Remediation
- SI-3 System and Information Integrity | Malicious Code Protection
- SI-4 System and Information Integrity | System Monitoring
- SI-5 System and Information Integrity | Security Alerts, Advisories, And Directives
- SI-10 System and Information Integrity | Information Input Validation
- SI-12 System and Information Integrity | Information Management and Retention

5. Texas DIR Data Classification Guide

The College's Office of Cybersecurity and the Texas Department of Information Resources (Texas DIR) worked with a taskforce of agency stakeholders to develop the Texas DIR Data Classification Guide, which is a model data classification taxonomy for state agencies and institutes of higher education.

Data Classification is the process of categorizing data into various types, forms, sensitivity level, or any other grouping of similar characteristics. When a piece of information (e.g., a document, memo, or customer record) is created, the Information Owner assigns a standard classification level which defines the prescribed handling requirements for that piece of information. Such categories dictate the controls necessary to best protect the Confidentiality, Integrity, and Availability of the data.

College data stored, processed, or transmitted using College Information Resources or other resources where College Business occurs is required to be classified into categories as described by the Texas DIR Data Classification Guide into one of the following four (4) categories:

a. **Regulated** focuses on the types of data typically regulated by federal statute or third-party agreements. Agencies, including the College, that maintain protected health, federal tax, payment card, or certain personal information will have specific requirements placed on that data by a non-Texas regulation. Therefore, regulated data has specific handling requirements that are unique to their regulations and do not apply to all agencies. The category "Regulated" is protected specifically by Federal or State law or College Policy and Procedures, including but not limited to HIPAA, FERPA, PC-DSS, Gramm-Leach-Bliley, and the Texas Identity Theft Enforcement and Protection Act.

b. **Confidential** is the highest level of classified data at the College. A breach of Information Resources classified as Confidential would cause exceptionally grave damage to the mission of the College. The Confidential label is used to identify information that is typically excepted from public disclosure, whether specified in law or through a decision by the Open Records division of the Texas Office of the Attorney General. Confidential data include information such as attorney-client communications, protected draft communications, and computer vulnerability reports that is typically exempted from the Public Information Act and includes the data commonly referred to as "Regulated" data. College data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring Confidentiality, Integrity, or Availability considerations (e.g., Non-Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.). Data defined in Texas Business and Commerce Code § 521.002(a)(2) is included. Examples of Confidential data may include but not limited to:

   - Personally Identifiable Information (PII): SSN, DOB, Account Numbers
   - Intellectual property: Vendor copyrights, patents, or trade secrets.
   - Passwords
   - Network architecture schematics and diagrams.

c. **Sensitive Data** is controlled College data that is not otherwise identified as Confidential data, but which is releasable in accordance with the Texas Public Information Act (e.g., contents of specific e-mail, date of birth, salary, etc.) Such data must be appropriately protected to ensure a controlled and lawful release. A breach of College data classified as Sensitive would cause damage to the mission of the College. Information that could be subject to release under an open records request but should be controlled to protect third parties. Examples of Sensitive Data may include but not limited to:

   - Operational information
   - Personnel records
   - Information Security procedures
   - Research

- Internal Communications

d. **Public Data** is all other data that is not Confidential and is therefore subject to public disclosure pursuant to the Texas Public Information Act. The Public information label is used for information such as published reports, press releases, and information published to the agency's public website. Such information requires no authentication and is freely distributable by all agency personnel. This data is not otherwise identified as Confidential or Sensitive data. Such data has no legislative requirement for confidentiality, integrity, or availability and is freely and without reservation made available to the public.

6. Roles and Responsibilities

The roles and responsibilities as defined by the Information Security Program are described in Procedure III.3010.A.a, Information Security Program. Described below are specific responsibilities that pertain to this Procedure.

a. **All College Users** are:

- Required to read and acknowledge the College's **Procedure III.3010.A.f, Acceptable Use of Information Resources** in exchange for the User being granted access to Information Resources and Protected Data.
- Expected to fully cooperate in any investigation of Information Resource abuse. The User agrees to follow all directives from the Chancellor or Designee, whether communicated verbally, in writing, or other media.
- Must immediately report suspected breaches, theft, and incidents associated with College data to Technical Support and the CISO. Technical Support: ITS Technical Support can be contacted by email at TechSupport@sjcd.edu or by phone at (281) 998-6137.

b. **Users who are elected officials, employees, and contractors** are:

- Required to complete Annual Cybersecurity Training Program. Users who are elected officials, employees, and contractors that use a computer to complete their College job responsibilities are required to complete an annual cybersecurity training program as certified by Texas Department of Information Resources (Texas DIR). Such Users agree and understand that access to College Information Resources is subject to their completion of annual cybersecurity training.

c. **Information Owners and Information Custodians**. Based on the Data Classification determined for an Information Resource, the Information Owner and the Information Custodian of the Information Resource are required to implement:

- Appropriate security controls as defined by Texas DIR Security Controls Standard Catalog.
- Records retention procedures as defined by Texas State Library and Archives Commission's (TSLAC) and the Office of Records Management. Information Owners and Information Custodians may seek additional guidance from The Office of Cybersecurity (OCS) and Information Technology Services (ITS) if unsure of which controls are necessary for the data under their responsibility.

7. College data and Personal Devices

College Business related data stored, processed, or transmitted using a Personal Device is subject to College Policies and Procedures.

8. Personal Data

Personal Data, being data that is personal to the User and stored, processed, or transmitted using College Information Resources as a result of incidental personal use is not considered College data and is excluded from this Procedure.

9. Definitions

The terms referenced in this Procedure are outlined in **Procedure III.3010.A.a, Information Security Program**, Section 14. Definitions**.**

Note: See **Procedure III.3010.A.b, Cybersecurity Risk Management** for additional information on cybersecurity.

Date of SLT Approval	February 15, 2024
Effective Date	February 15, 2024
Associated Policy	Policy III.3010.A, Information Resources
Primary Owner of Policy Associated with the Procedure	Chief Technology Innovations Officer
Secondary Owner of Policy Associated with the Procedure	Chief Information Security Officer.