# Overview

## Purpose

The purpose of this standard is to provide the SDCC community with a framework for securing information from risks including, but not limited to, unauthorized use, access, disclosure, modification, loss, or deletion. This standard defines the controls required for handling all University managed information with the goal of identifying the classifications of information handled as well as defining the requirements for handling different levels of sensitive information.

Information must be classified by its sensitivity, criticality, and associated risks as required by the University's Information Security Plan. Classification of information is essential for determining the baseline security controls for the protection of data.

## Audience

This standard applies equally to any individual who creates, uses, processes, stores, transfers, administers and/or destroys SDCC information, regardless of the environment or media on which the information resides. SDCC information includes but is not limited to information about students, former students, employees, research data, and intellectual property.

## Definitions

**Confidential Data**: Generalized term that typically represents information classified as confidential according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.

**Institutional Data**: All data owned or licensed by the University, including research data.

**Information Asset**: Definable pieces of information that are recognized as “valuable” to the University.

Non-public Information: Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

## Standard Detail

The goal of information security, as stated in the SDCC Information Security Plan, is to protect the confidentiality, integrity and availability of information assets and systems. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. Information assets and systems are classified according to the risks associated with the data being stored or processed. High risk data needs the greatest amount of protection to prevent compromise while lower risk data can be given proportionately less protection. There are also specific laws and regulations that govern certain kinds of data. All institutional data should be classified into one of three classification or (tiers):

### Tier I—Confidential Data

Data is classified as Tier I—Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the college or its affiliates. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied.

Tier I—Confidential data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high.

Examples of Tier 1—Confidential data include official student grades and financial aid data, social security and credit card numbers, research data, and individuals' health information.

#### Examples of How Data Can Be Lost

- Workstation with access to data and systems is compromised.
- User account with access to data is compromised.
- Unsecured network service or application is compromised, and data stolen.
- Mobile device such as a laptop or smartphone is lost or stolen.
- Former employee accesses system because "shared" passwords were not changed.
- Unauthorized visitor walks into an office or lab and steals equipment.
- Unauthorized user accesses an unsecure computer.

#### Impact of Tier I Data Loss

- Long-term loss of all federal funding including financial aid
- Long-term loss of reputation.
- Published research called into question because data is unreliable.

- Increase in regulatory requirements.
- Civil monetary penalties as well as imprisonment.
- Long-term loss of critical college service(s) such as accepting credit cards payments.
- Individuals put at risk for identity theft.

## Tier II—Internal/Private Data

Data should be classified as Tier II—Internal/Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the college or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data and a reasonable level of security controls should be applied.

Tier II—Internal/Private Data is considered moderately sensitive in nature. The risk for negative impact on the college should this information not be available when needed is typically moderate.

Examples of Internal/Private data include official university records such as financial reports, non-PII human resources information, some research data, unofficial student records, and budget information.

### Examples of How Data Can Be Lost

All the examples detailing how Tier 1 data can be lost are applicable. Tier 2 data in some cases is also more susceptible to unauthorized disclosure as employees are more likely to release the data by mistake or due to being the victim of a social engineering attack.

### Impact of Tier II Data Loss

- Short-term loss of reputation.
- Short-term loss of federal or research funding.
- Short-term loss of critical departmental service.

## Tier III—Public Data

Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the college and its affiliates. While little or no controls are required to protect the confidentiality of Tier III—Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Tier III Public data is not considered sensitive however the integrity of Public data should be protected. The impact on the institution should Tier III - Public data not be available is typically low (inconvenient but not debilitating). Examples of Public data include directory information, course information, and research publications.

**Examples of How Data Can Be Lost**

Most of the examples listed for Tier I data apply.

**Impact of Tier III Data Loss**

- Loss of use of personal workstation or laptop.
- Loss of personal data with no impact to the University.
- Publicly accessible data could be inaccurate due to unauthorized modification.
- Publicly accessible data could be modified to direct users towards malicious systems.

## Data Handling

Records containing confidential information should exist only in areas where there is a legitimate and justifiable business need. Confidential information should be accessed from its original source whenever possible. Copies and printed versions of the information should be kept to a minimum.

## Access

Access to Confidential data must be controlled from creation to destruction and will be granted only to those persons affiliated with the college who require such access in order to perform their job (need to know basis). Access to Confidential data must be individually requested and then authorized by the Data Owner who is responsible for the data.

Access to Internal/Private data must be requested from, and authorized by, the Data Owner who is responsible for the data. Access to Internal/Private data may be authorized to groups of people by their job classification or responsibilities (role-based access) and may also be limited by one's department.

Employees should receive annual training on their responsibilities regarding appropriate use and steps they can take to protect University confidential information. Employees with access to confidential information should be reviewed on an annual basis to ensure that access to this information is still needed. The list of people who have access to confidential information and evidence of annual review of their access shall be made available for audit purposes

## Use, Transmission, and Storage

The following controls are required when using, transmitting, or storing confidential information:

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.
- When printing, photocopying, or faxing, ensure that only authorized personnel will be able to access the output. Sensitive information should not be transmitted to network-connected printing/scanning devices unless on a closed or securely encrypted network.
- All confidential data must be stored only on centrally managed network storage devices. Confidential data cannot be stored on any local storage devices under any circumstances.
- Proprietary research equipment or instruments that are unable to reasonably output data to the centrally managed network storage devices must have a periodic backup mechanism that copies the output data onto a centrally managed network storage device.
- Store paper documents in a locked drawer and in a locked room or other secure location.
- Confidential information may not be stored on any personal equipment. Additionally, users may not send or forward emails containing Tier I data to personal email accounts.
- Properly identify such information as Confidential to all recipients by labeling it accordingly, providing training to personnel, explicitly mentioning the classification or similar means.
- Encrypt sensitive information when (1) placing it on removable media; (2) placing it on a mobile computer (e.g. laptops, PDAs, smart phones); or (3) sending it via electronic mail.
- Do not send sensitive information via instant message or unsecured file transfer.

## Destruction

SDCC records should be destroyed only in accordance with the college's records retention schedule. Sensitive information in electronic form should be destroyed using industry standard software wiping or degaussing technology. Deleting files or reformatting electronic media is not sufficient for data destruction.

Sensitive information on paper should be pulped or crosscut shredded, including all transitory work products such as unused copies, drafts and notes.

## Breach Disclosure of Sensitive Information

Please report any information security problems or potential problems immediately. Timely reporting will help determine if further investigation is necessary and can limit further damage or loss of data. Please see the IT Incident Response Procedure for further reference.

## Consequences and Sanctions

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other college rules and regulations including progressive discipline up to and including that which is allowed under the CBA.

## Appendix A: Predefined Types of Confidential/Restricted Information Assets

Based upon state, federal, and contractual requirements that SDCC is bound by, the following information assets have been predefined as Tier I or Tier II data and must be protected. If you have questions about the appropriate classification for any information not specifically mentioned below, please contact the ithelp@sdccd.edu.

### Personally Identifiable Education Records—Covered under FERPA

Personally identifiable education records are defined as any education records that contain one or more of the following personal identifiers:

- Student M number
- Grades, GPA, credits enrolled
- Social Security Number (SSN)
- Race/gender
- A list of personal characteristics or any other information that would make the student's identity easily traceable
- Personally Identifiable Financial Information—Covered under GLBA

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- Date of birth

- Financial account number in combination with a security code, access code or password that would permit access to the account

**Export Controlled Research—International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)**

Export controlled research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism, or non-proliferation. This kind of data cannot be stored on systems outside the United States nor can non-US Citizen's work on this type of project. Examples include:

- Chemical and biological agents
- Scientific satellite information
- Military electronics and nuclear physics

**Payment Card Information—Covered under PCI DSS**

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card’s magnetic stripe

**Protected Health Information (PHI)—Covered under HIPAA**

PHI is defined as any individually identifiable information* that is stored by the University. PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone/fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers

- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol(IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

*If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered individually identifiable and therefore would not be considered PHI.