# ADMINISTRATIVE REGULATION 3726

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

GENERAL INSTITUTION

## INFORMATION SECURITY-DATA CLASSIFICATION

### I. PURPOSE AND SCOPE

The purpose of this administrative regulation is to provide information security requirements for ownership, classification, and protection of the South Orange County Community College District (SOCCCD) information assets.

An information asset is a definable piece of information, regardless of format, that is recognized as valuable to the organization. Classifying information is at the core of an information security program because it specifies how information, based on its sensitivity and value, will be protected from unauthorized disclosure, use, modification or deletion.

This is one of a series of information security administrative regulations maintained by the District Information Technology (IT) department designed to protect SOCCCD information systems.

Please refer to *AR-3725 – Information Security Program Overview* for applicability of assets, application to staff, and external parties.

### II. RESPONSIBILITIES

The following roles and responsibilities are established for carrying out this data regulation:

A. Executive sponsors are senior college officials who have planning responsibility and accountability for major administrative data systems (e.g. student, human resources, financial, research, etc.) within their functional areas. By understanding the planning needs of the institution, they are able to anticipate how data will be used to meet institutional needs.

B. Data stewards are appointed by the executive sponsors to implement established data policies and general administrative data security policies for their functional areas. Data stewards are responsible for safeguarding the data from unauthorized access and abuse through established security and authorization procedures and educational programs. They authorize the use of data within their functional areas and monitor this use to verify appropriate data access. They support access by providing appropriate documentation and training to support data users. Data stewards, having served informally at the institution, will be identified and serve on existing change management committees and the District and/or campus information security team as appropriate.

C. Data owners are employees who most often report to data stewards and whose duties provide them with an intricate understanding of the data in their area. They work with the data stewards to establish procedures for the responsible management of data, including data entry, auditing and reporting. Some data administrators may work in a technology unit outside of the functional unit, but have responsibilities such as security and access as decided by the stewards. Technical data administrators may also be responsible for implementing backup and retention plans or ensuring proper performance of database software and hardware. Data administrators, having served informally at the institution, will be identified and called upon for their subject matter expertise.

## III. DATA CLASSIFICATION

Users of SOCCCD systems need to understand the importance of securely handling the information they are able to access and the standards that have been created to ensure data protection. For the purposes of this administrative regulation, data includes both electronic and paper.

Specific protection requirements are mandated for certain types of data, such as credit card information, personally identifiable information, or financial data. Where information is entrusted to us by our students, employees, or business partners, their expectations for secure handling must be met. Consistent use of this administrative regulation will help to ensure that we maintain adequate data protection.

### A. Classification of Data Assets

SOCCCD classifies information regardless of medium (electronic or paper) according to its sensitivity and the potential impact of disclosure.

In general, information is disclosed to employees or others when there is a business need-to-know. Information must be consistently handled according to its requirements for confidentiality and disclosure.

Data Owners, defined below, are responsible for determining the appropriate classification level for data for which they are responsible or for the same information maintained on paper documents.

If the classification level is set too high, the cost of protection will be excessive in relation to the value or sensitivity of the data. If it is set too low, the risk of compromise could be increased. Downgrading to a lower classification at a future date is appropriate should conditions warrant.

### B. Data Ownership

Every business application must have one or more designated Data Owners. The Data Owner is the person responsible for (or dependent upon) the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, or otherwise processed, and is therefore best suited to make decisions about the information on behalf of the organization.

The Data Owner is ultimately responsible for security decisions regarding the data. The Data Owner will work with the appropriate college Technology Departments or District Information Technology (IT) department to ensure that minimum-security standards are met. The District IT and college Technology departments will provide appropriate security technology solutions (such as system or application security controls or encryption methods) based on classification level.

If the Data Owner has chosen to outsource processing or storage of information at a location outside of SOCCCD's control, such as on a cloud-based service, the Data Owner retains full accountability for security of the information. Security controls that are required to be performed by the third-party service provider must be detailed in the contract with that provider, and monitored by the Data Owner.

The Data Owner's responsibilities include:

1. Classifying data for which they are responsible. This includes determining the level of confidentiality that should be assigned to information, which will dictate its level of protection;
2. Working with IT to select security controls that are appropriate to the level of sensitivity, value or confidentiality of the application or data it processes;
3. Ensuring that third parties to whom data has been entrusted meet SOCCCD security requirements;
4. Establishing and maintaining response plans which identify actions to be taken for their area of control, such as Security Incident Response processes and defined Business Continuity Plans; and
5. Depending on location, provide District and/or College IT management with administrative access in order to maintain continuity of access to systems and services.

C. Data Classification Categories

Information that is owned, used, created or maintained by SOCCCD must be classified into one of three categories:

1. Public

   Data classified as Public is suitable for routine public disclosure and use. Security at this level is the minimum required by SOCCCD to protect the integrity and availability of this data. Examples of this type of data include, but are not limited to, data routinely distributed to the public such as publicly accessible web pages, marketing materials, and press statements.

2. Internal

   Internal data is information about SOCCCD or internal processes that must be guarded due to proprietary or business considerations, but which is not personally identifiable or otherwise considered confidential. This classification may apply even if there are no regulatory or contractual requirements for its protection.

   Data in this category is generally available to employees, contractors, students, or business associates, but is not routinely distributed outside SOCCCD. Some Internal data may be limited to individuals who have a legitimate business purpose for accessing the data, and not be available to everyone. Examples of Internal data may include:

- SOCCCD procedures and manuals
- Organization charts
- Data which is on the internal Intranet (SharePoint), but has not been approved for external communication
- Software application lists or project reports
- Building or facility floor plans or equipment locations

3. Restricted

- Restricted data is information that is sensitive in nature, and may be proprietary, personally identifiable, or otherwise be sensitive. Unauthorized compromise or disclosure of the information would be likely to cause serious financial, legal, or reputation damage to SOCCCD, or result in embarrassment or difficulty for SOCCCD, its employees, or students. Restricted data may be protected by statutes, regulations, or contractual requirements. Disclosure is limited to those within SOCCCD on a "need-to-know" basis only. Disclosure to parties outside of SOCCCD must be authorized by appropriate management and covered by a binding confidentiality or non-disclosure agreement. Examples of Restricted data include: personally identifiable (as defined below) information of our employees, contractors, or students.
- Human Resources, employee or payroll records.
- Student data.
- Specialized audit reports or results.
- System and network configuration details, including diagrams, passwords, programs or other IT-specific documentation.
- Intellectual property.
- Health records.
- Legal documents.

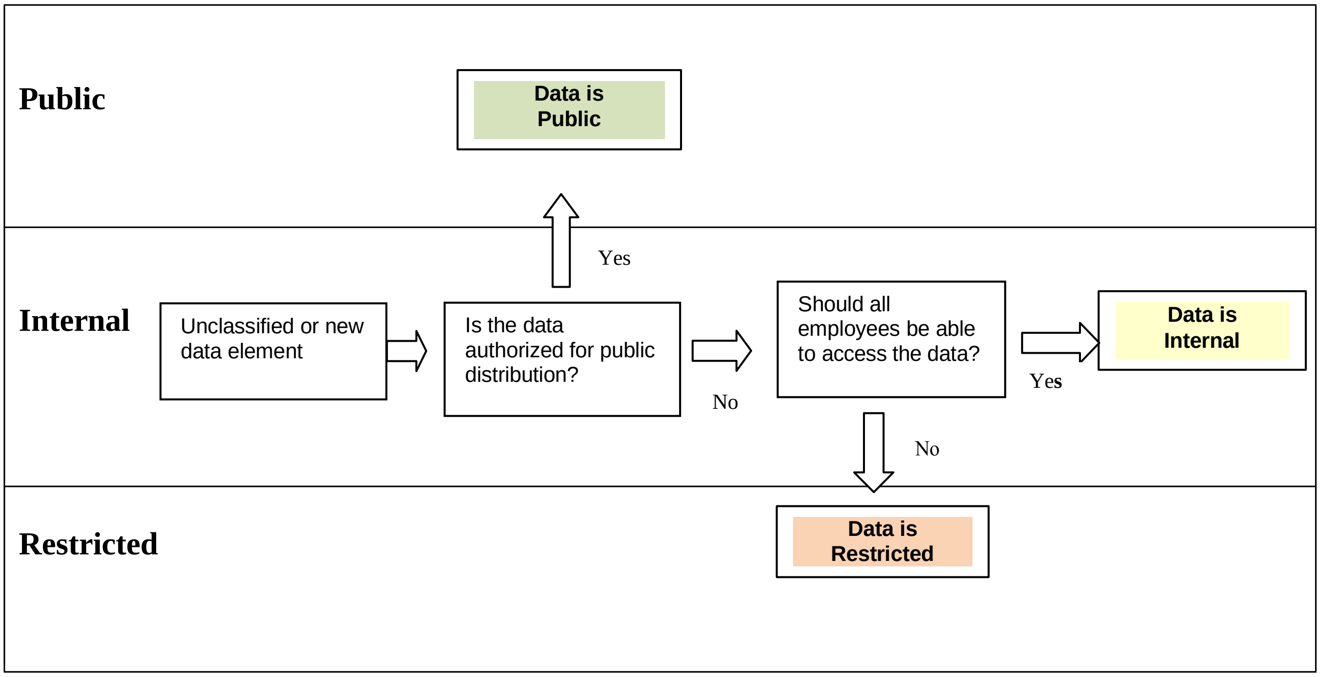
For purposes of this administrative regulation, the term "personally identifiable information" means an individual's first name and last name or first initial and last name in combination with any one or more items of personal information, such as social security number or other identity verification number, driver's license number or state-issued identification card number, student and/or employee ID numbers, financial account number, credit or debit card number, date or place of birth, and gender or gender identity; provided, however, that "personally identifiable information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

D. Minimum Classification

All information should be assumed *Internal* unless classified otherwise.

E. Classification Flow Chart

The Classification Flow Chart below is intended to assist a Data Owner, document creator or user to assist in quickly determining the classification of a data element or document.


Public
Data is Public
Internal
Unclassified or new data element
Is the data authorized for public distribution?
Yes
No
Should all employees be able to access the data?
Yes
Data is Internal
No
Restricted
Data is Restricted

F. Information Access

The Data Owner makes access decisions regarding information they are responsible for, and must be consulted when access decisions are to be made, extended, or modified. Please refer to *AR-3727-Information Security–Access Control* for additional information.

G. Periodic Review

The Data Owner at least every two years, or when necessary based on business need must review information asset classifications. Review records must be maintained by Data Owners documenting the review processes took place.

*Reference:*

*Civil Code 1798.29*
*Family Education Rights and Privacy Act (FERPA)*
*Social Security Number Policy*
*Health Insurance Portability and Accountability Act (HIPAA)*