Information Security - Data Classification

1. Purpose and Scope

The purpose of this Administrative Regulation is to provide information security requirements for ownership, classification, and protection of Yosemite Community College District (YCCD) 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 Services (ITS) department designed to protect YCCD information systems.

2. Data Classification

Users of YCCD 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 (AR), 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 Data Classification Administrative Regulation will help to ensure that we maintain adequate data protection.

2.2 Classification of Data Assets

YCCD 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.

2.1 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 campus or District ITS department to ensure that minimum security standards are met. ITS 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 YCCD'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:

- 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.
- Working with ITS to select security controls that are appropriate to the level of sensitivity, value, or confidentiality of the application or data it processes.
- Ensuring that third parties to whom data has been entrusted meet YCCD security requirements.
- 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.
- Depending on location, provide District ITS management with administrative access in order to maintain continuity of access to systems and services.

2.3 Data Classification Categories

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

- Public
- Internal
- Restricted

2.3.1 Public

Data classified as *Public* is suitable for routine public disclosure and use. Security at this level is the minimum required by YCCD 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.

2.3.2 Internal

Internal data is information about YCCD 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 YCCD. 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:

- YCCD 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

2.3.3 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 YCCD, or result in embarrassment or difficulty for YCCD, its employees, or students. *Restricted* data may be protected by statutes, regulations, or contractual requirements. Disclosure is limited to those within YCCD on a "need-to-know" basis only. Disclosure to parties outside of YCCD must be authorized by appropriate management and covered by a binding confidentiality or non-disclosure agreement.

Examples include:

- Personally identifiable (as defined below) information of our employees,

contractors, or students
- HR, employee or payroll records
- Student data
- Audit reports or results
- System and network configuration details, including diagrams, passwords, programs or other ITS 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; 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.

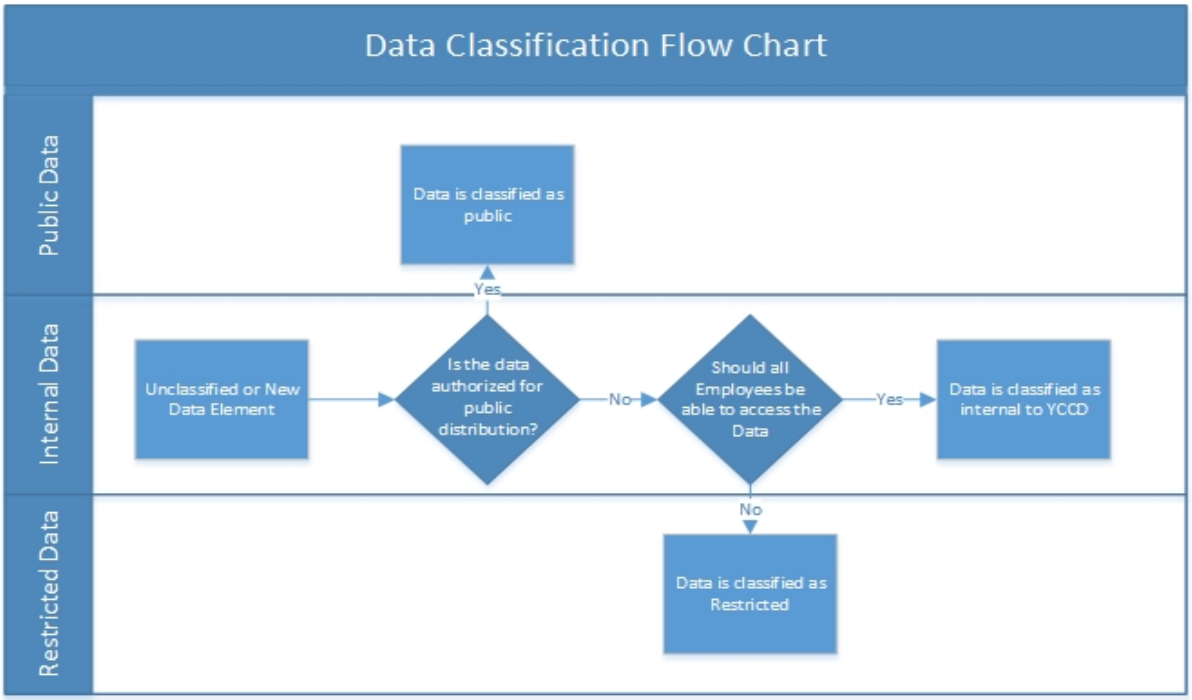
2.4 Minimum Classification

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

2.5 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.

Information Security - Data Classification



2.6 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.

2.7 Periodic Review

The Data Owner must review Information assets classifications at least every two years, or when necessary based on business need. Records must be maintained by Data Owners documenting the review processes for audit purposes.

Authority

This Administrative regulation was created and adopted under the authority of the Assistant Vice Chancellor of Information Technology Marty Gang YCCD (Yosemite Community College District).

Related Laws, Regulations and Policies

California Community Colleges Information Security Center
CCC Data Classification Standard

Federal Legislation and Guidelines
Electronic Communications Privacy Act of 1986 (ECPA)
Family Educational Rights and Privacy Act of 1974 (FERPA)