RHODE ISLAND COLLEGE **OFFICIAL POLICY**	***Data Classification***	**EFFECTIVE DATE/REVISION HISTORY** *Original policy adopted 2025/07/24*
RESPONSIBLE OFFICE: *Information Technology Services*	**POLICY OWNER:** *Information Technology Services, Institutional Research & Data Governance Committee*	**LINK TO HOME PAGE OF RESPONSIBLE OFFICE**

PART 1. RATIONALE

Information technology and data constitute valuable Rhode Island College assets. The purpose of data classification is to identify college data and its sensitivity. In order to protect the security, confidentiality and integrity of Rhode Island College data (referred to as “College Data”) from unauthorized access, modification, disclosure, transmission or destruction, as well as to comply with applicable state and federal laws and regulations, all College Data must be classified within security levels, with regulations on the usage, storage, disposal, and access of data at each level.

To effectively secure College Data, we must have a shared vocabulary that we can use to describe the data and quantify the amount of protection required. This policy defines four (4) categories into which all College Data can be divided:

- Public
- Internal
- Confidential
- Restricted Use

Data Classification Reference Chart

PART 2. SCOPE

College-wide - Any College Data residing on any medium. This includes, but is not limited to college-owned or personal laptops, desktops, servers, handheld devices, external drive, mobile device, and paper.

PART 3. DEFINITIONS [as used in this document]

Data Classification	The process of organizing data into four (4) categories for ease of retrieval, sorting, and storing for future use, with the primary purpose of helping the college determine risk tolerance across all its data assets.
Information Privacy and Security Laws	Federal and state laws that classify data and/or establish specific requirements regarding data/information security. Examples include, but are not limited to, the Family Educational Rights and Privacy Act (FERPA), the Health Information Portability and Accountability Act of 1996 (HIPAA), and GLBA Safeguards Rule.

Institutional or College Data	Refers to data elements that are relevant to the operations, plans, or management of a RIC academic, financial, or administrative unit, or used in reporting, decision-making, business, or administrative processes. This includes data that falls under information privacy and security laws or regulations (ex. FERPA, HIPAA, GLBA Safeguards Rule etc.) and may be created at the College or imported through various processes into college data systems.
Unauthorized Access	Refers to an individual gaining logical or physical access without permission to a network, system, application, data, or other resource.
Data Access	The ability to access data via systems, reports, shared folders, paper, etc. Data access must be determined by role (on a "need to know" basis), with the approval of the appropriate data steward.
Risk Management	The systematic process of identifying, assessing, and mitigating potential threats that could compromise the confidentiality, integrity, and availability of an organization's data, by analyzing the likelihood of these threats occurring and the potential impact they could have, and then implementing appropriate security measures to minimize those risks.
Information Systems	The combination of hardware, software, networks, databases, paper-based records, and associated processes that are used to collect, process, store, manage, and transmit data within the college. These systems include both digital and physical infrastructures that support college operations, such as administrative systems, learning management systems, research systems, communication platforms, and paper-based record-keeping methods.

PART 4. STATEMENT OF POLICY

The college will use data classification to develop other policies and guidelines for risk-based protection of information systems. Data classifications are based upon the expected risk of harm to individuals and the college if the data were to be subject to unauthorized access, use, modification, disclosure, deletion, and/or destruction.

DATA CLASSIFICATION LEVELS

To implement security measures at the proper level, establish guidelines to meet legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data. The data will be classified into one of the four levels described below and must be collected, transmitted, stored, or displayed in means appropriate to that level of classification.

1. Level 4 – Restricted (Red)

This data classification level is for data that is **high risk** because it is sensitive data that is highly confidential in nature. The loss of the data's confidentiality, integrity, or availability will cause exceptionally grave damage to RIC's mission, safety, finances, or reputation. Privacy and security for this data classification are typically required by law or contract. Access to this type of data must require authorization from appropriate data steward and legitimate need-to-know by college employees.

Examples include but are not limited to: Protected Health Information (PHI) data, Personally Identifiable Information (PII) data, Payment Card Industry Data Security Standard (PCI DSS) data, Gramm-Leach-Bliley Act (GLBA) data, Controlled Unclassified Information (CUI)data, Federal Information Security Management Act (FISMA) regulated data, and information protected by non-disclosure agreements. For additional information, see Data Classification Reference Chart.

2. Level 3 – Confidential /Sensitive (Orange)

   This data classification level is for data that is **moderate risk** because it should be kept confidential. The loss of the data's confidentiality, integrity, or availability can cause harm to RIC's mission, safety, finances, or reputation. Privacy and security for this data classification level may be required by law or contract. Access to this type of data must require authorization from appropriate data steward and legitimate need-to-know by college employees.

   Examples include but are not limited to: Family Educational Rights and Privacy Act (FERPA) data, proprietary business plans, patent pending information, personnel records, login credentials, non-public contracts, and intellectual property. For additional information, see Data Classification Reference Chart.

3. Level 2 – Internal Use (Yellow)

   This data classification level is for data that is **low risk** and includes information that is not openly shared with the public but is not specifically required to be protected by statute or regulation. The loss of the data's confidentiality, integrity, or availability will not directly cause harm to RIC's mission, safety, finances, or reputation, contractual, or regulatory violations, but might otherwise cause unintended/unnecessary/unfavorable impact to the college, individuals, or affiliates.

   Note: While some forms of internal data can be made available to the public, this data classification is not freely disseminated without appropriate authorization from respective data steward and/or management and senior leadership.

   Examples include but are not limited to: budgetary plans, salary information, personal cell phone numbers, departmental policies and procedures, internal memos, unpublished research, routine business records. For additional information, see Data Classification Reference Chart.

4. Level 1 – Public Use (Green)

   This data classification is for data that is **minimal risk**. The loss of the data's confidentiality, integrity or availability will not likely cause harm to RIC's mission, safety, finances, or reputation, and the college has chosen or is required to disclose it to the public.

   Examples include but are not limited to: public directory, course catalogs, public research findings, enrollment figures, public websites, general benefits data, press releases, and newsletters. For additional information, see Data Classification Reference Chart.

DATA SECURITY MEASURES

Measures implemented for data security will be dictated by the data-classification level. Measures will include an appropriate combination of the following:

- Encryption
- Multi-Factor Authentication (MFA)
- Data protection
- Access control
- Documented backup and recovery procedures

- Change control and process review
- Data-retention
- Data disposal/destruction
- Audit controls
- Storage locations
- User awareness

PART 5. PROCEDURES

College employees, or others who are associated with the college, who request, use, possess, or have access to college data must agree to adhere to the protocols outlined above. In addition, trustees, stewards, managers, and data users are prohibited from:

- Changing data about themselves or others except as required to fulfill one's assigned college duties or as authorized by the appropriate data steward and/or direct supervisor. (This does not apply to self-service applications that are designed to permit you to change one's own data.)
- Using information to enable actions by which other individuals might profit.
- Disclosing information about individuals without prior authorization by a supervisor.
- Engaging in what might be termed "administrative voyeurism" (reviewing information not required by job duties) unless authorized to conduct such analyses. Examples include tracking the pattern of salary raises, viewing a colleague's personal information and looking up someone else's grades.
- Circumventing the level of data access given to others by providing access that is broader than that available to them, unless authorized. For example, providing an extract file of employee salaries to someone who does not have security access to salary data is prohibited by this policy.
- Allowing unauthorized access to RIC's administrative systems or data by sharing an individual's username and password.
- Engaging in any other act that violates the letter and spirit of the policy, either purposefully or accidentally.

PART 6. ROLES AND RESPONSIBILITIES

Rhode Island College owns its College Data. Individual executive officer areas, units, and departments have stewardship responsibilities for portions of that data. Several roles govern the management of, access to, and accountability for institutional data. These roles include:

Role	Responsibilities
Data Trustee – VP Level	Have the ultimate responsibility and ownership of the data and systems
Data Steward	Any administrative personnel with policy-level responsibility for managing a major area (department) of the college's information resources. The Data Stewards design policies and procedures for their respective areas.
Delegated Data Steward	Senior college officials with policy-level responsibility that have been designated by a data steward to serve as the delegated authority for a specific data area. The responsibilities of delegated data stewards are the same as those for data stewards.
Data Manager	College officials and their staff that have operational-level responsibility for the capture, maintenance, and dissemination of data for specific data areas.
Data User	College departments, individual college community members, or college affiliates that have been granted access to College Data in order to conduct college business. Data users should understand the data classification level of the data with which they interact.

See **Data Stewardship Roles and Responsibilities** for a full list of responsibilities for each role.

PART 7. CONTACTS

Subject	Office or Position	Telephone Number	Email
Policy Clarification	Assistant Vice President/Chief Information Officer	(401) 456-8897	avpis@ric.edu
Policy Clarification	Dir. Institutional Research & Planning	(401) 456-8998	irpo@ric.edu

PART 8. POLICY ENFORCEMENT

Violation(s)	Accessing data to which you do not have permission or sharing data in ways not consistent with its classification.
Potential consequences	Failure to comply with this policy puts the College and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).
Where to report violations	The Data Governance Committee

PART 9. FORMS/TEMPLATES/REFERENCE DOCUMENTS

Form, Template, or Document
Data Steward Roles and Responsibilities
Data Stewardship Matrix
Data Classification Reference Chart
Parent Policy: Data Governance