RHODE ISLAND COLLEGE	Information Handling Guide
March 24, 2025	Version 0.1

Contents

PURPOSE

The Rhode Island College Information Handling Guide serves as a cornerstone for maintaining the integrity, confidentiality, and availability of information assets within the organization. It provides clear procedures and protocols designed to ensure that all information, irrespective of its form or classification, is managed securely and effectively.

This guide equips every member of the organization with the knowledge and expectations necessary for the proper treatment of information, fostering a culture of shared responsibility for information security. By adhering to the principles outlined herein, the organization safeguards its reputation, complies with regulatory and contractual obligations, and protects against threats and vulnerabilities.

Key Features of this Guide:

- **Structured Classification System**: Information is categorized based on sensitivity and potential impact to enable the application of tailored security measures and handling protocols.
- **Comprehensive Coverage**: It addresses diverse information scenarios, including electronic and physical storage, data transmission, access control, and secure disposal.
- **Roles and Responsibilities**: Clear accountability is defined for all stakeholders, from senior leadership to individual employees, emphasizing a shared commitment to information security.
- **Commitment to Continuous Improvement**: This guide is a living document, regularly reviewed and updated to reflect advancements in technology, evolving business needs, and regulatory changes.

Through the adoption and implementation of this guide, the organization reaffirms its dedication to protecting valuable information assets and ensuring operational excellence in the face of modern security challenges.

SCOPE

This guide applies to all individuals, entities, and assets involved in handling the organization’s information, ensuring a consistent and secure approach across all operations.

Applicability

- **Personnel**: All employees, contractors, and temporary staff, as well as third-party partners, vendors, and other external entities who access or process organizational information.

- **Organizational Units**: All division and departments of the college.

Information Types

The guide encompasses all forms of information, including:

- **Internal Communications**: Emails, memos, and non-public announcements.
- **Employee and Student Data**: Personally identifiable information and service details.
- **Financial Records**: Accounting data, payroll information, and budgets.
- **Employee Personal Information**: HR records, benefits, and performance data.
- **Proprietary Information**: Research and development projects.
- **Public Information**: Marketing materials, press releases, and content approved for public dissemination.

Assets and Media

The guide applies to:

- **Electronic and Physical Assets**: Computers, servers, mobile devices, and hard copies.
- **Information Systems**: Databases, applications, and communication platforms.
- **Data Transmission Channels**: Email, file-sharing tools, and physical courier services.

Information Lifecycle

This guide governs every phase of the information lifecycle, referencing the **Information Classification Policy** and the **Information Handling Guide**:

- **Creation and Classification**: Assign sensitivity levels based on organizational standards.
- **Storage and Access**: Apply security controls appropriate to classification levels.
- **Transmission**: Ensure secure internal and external sharing of information.
- **Retention and Disposal**: Adhere to established retention schedules and secure destruction protocols.

ROLES AND RESPONSIBILITIES

Effective information handling relies on the collaboration and accountability of all stakeholders within the organization. The following roles outline key responsibilities:

Senior Leadership

- Establish and promote the organization's information classification program and this guide.
- Foster a culture of security awareness and lead by example.
- Ensure compliance with legal, regulatory, and ethical standards.
- Allocate resources to ensure compliance with classification policies and support enforcement measures.

Information Security Officer

- Oversee the development, implementation, and enforcement of the Information Classification Policy and this guide.
- Ensure that classification guidelines align with business objectives, security needs, and legal requirements.
- Conduct periodic reviews to assess compliance and update classification policies as needed.
- Provide leadership in responding to data security incidents related to classification compromises.
- Ensure correct application of classification labels across all formats (electronic documents, databases, emails, and printed materials).
- Provide training and guidance to employees on accurately classifying and marking sensitive data.
- Enforce classification policies to prevent unauthorized disclosure or mishandling of restricted information.

IT Security Team

- Implement technical controls to enforce classification policies, such as access restrictions, encryption, and monitoring tools.
- Conduct security assessments to identify vulnerabilities in classification and handling processes.
- Respond to security incidents involving misclassified or improperly handled data.

Data Owners

- Assign classification levels to information assets based on sensitivity and regulatory requirements.

- Regularly review and update classifications, especially following changes in business operations, regulatory updates, or security risks.
- Ensure proper labeling and secure handling of classified information.

All Employees and Contractors

- Accurately classify and label information at the point of creation or modification.
- Follow classification handling procedures to ensure proper protection (e.g., encryption, secure storage, controlled access).
- Report any suspected misclassification, policy violations, or unauthorized data access incidents.

Third-Party Vendors and Partners

- Adhere to the organization's Information Classification Policy when accessing or processing classified data.
- Implement necessary security measures to protect classified information from unauthorized disclosure.
- Promptly report any security concerns or incidents involving classified information.

INFORMATION CLASSIFICATION

This section provides a concise overview of our organization's established Classification Program, as detailed in our Information Classification Policy. The program categorizes information into three primary classifications to guide the handling, sharing, and security of data across our operations. Each classification reflects the sensitivity of the information and dictates the required protective measures to safeguard it effectively. Here's a summary of the classifications:

Classification	Access	Attributes	Examples
Restricted	Access limited to personnel with express business purpose	Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial, or reputational harm to the organization, its staff and its constituents/people served.	Social Security number Banking information Health information Payment Card information Data flow diagrams

Classification	Access	Attributes	Examples
		Information required by outside party, via regulation or contract, to be safeguarded due to Confidentiality, Integrity, or Availability risks.	Security Control implementation descriptions Information system authentication information Passport and Visa numbers Federal Taxpayer Information (FTI)
Confidential	Access requires authorization from appropriate data steward and legitimate need-to-know by college employees.	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.	Family Educational Rights and Privacy Act (FERPA) data Proprietary business plans Patent pending information Personnel records Login credentials Non-public contracts Intellectual Property
Internal	Access and distribution limited to organization personnel; controlled business exceptions apply	Information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial, or reputational harm to the University, its staff and its constituents/people served	Internal organization Policy and Procedure documents HR employment records Unpublished Research data
Public		Information whose loss, corruption, or unauthorized	Marketing information

Classification	Access	Attributes	Examples
	Access and distribution not controlled	disclosure would cause minimal or no personal, financial, or reputational harm to the University, its staff and its constituents/people served	Promotional materials
			Published Research data
			Student and Public Policies

HANDLING RULES

Handling rules for information are dynamically applied based on the specific actions being taken with the information (such as storage, transmission, processing, or disposal) and the classification of that information. The overarching goal is to ensure that appropriate security measures are applied to protect the information from unauthorized access, use, disclosure, alteration, or destruction throughout its lifecycle. The essence of these handling protocols is distilled into two primary considerations:

- **The Nature of the Activity**: This refers to the actual processes or actions being performed with the information, such as transmission via email, reproduction through printing, storage on physical or cloud-based platforms, or the final disposal of the information. Each activity presents unique security challenges and requires tailored protective measures to mitigate risks effectively.

- **Information Classification**: The level of sensitivity and intended audience of the information significantly influences how it is managed. Classified into categories such as Public, Internal, and Restricted, each level demands a corresponding set of security protocols. Public information, designed for wide dissemination, requires minimal restrictions, whereas Internal and Restricted classifications necessitate progressively stringent security measures to uphold the confidentiality and integrity of the information.

<u>General Guidelines / Instructions</u>

- The approach to using this guideline is as follows:
  - Identify all the types of information one is handling and classify (see section Classification Rules)

  - Based on the classification, select what is done with the information (e.g, emailing, printing, etc., see list below).
  - Follow the handling instructions outlined

- Any information created or received by Rhode Island College employees in the performance of the employee's job at Rhode Island College is Internal, by default, unless the information requires a higher classification or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification to the combined asset. For example, if an application contains Public and Internal information, the entire application is classified as Internal.
- Restricted and Internal information must never be released to the general public but may be shared with third parties, such as government agencies, business partners or consultants, when there is a business need to do so and the appropriate security controls and contractual agreements are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.
- Federal Tax Information (FTI) includes any tax return or taxpayer information received directly from the IRS or obtained through authorized sources such as the Social Security Administration (SSA) and Federal Student Aid (FSA). Examples include names, addresses, Social Security Numbers, and other tax return data. For the purposes of data classification and handling, this information is Restricted.

Information Handling Standards:

This section outlines the specific handling rules for various types of information based on their classification. It includes standards for maintaining secure workspaces, managing email communications, storing files, handling hard copy documents, and using electronic devices. These rules ensure consistent and secure practices to protect Internal, Public, and Restricted information within the organization.

Service or Medium	Internal	Public	Restricted

Desk / Working Area	Follow Restricted guidelines.	Maintain a tidy and professional workspace.	Avoid leaving restricted information in plain view. Keep sensitive documents organized and secured when not in use.
Email	Follow Restricted guidelines.	Standard practices; professionalism encouraged.	Use Rhode Island College Microsoft Outlook. Label emails containing restricted information in the subject line or body of email, and avoid sending attachments. Prefer using links to stored documents. Ensure emails and attachments sent to external parties are encrypted.
File Storage **(Network Drives, Cloud Services)**	Follow Restricted guidelines.	Can be stored in general access areas without special encryption, but with regular monitoring for unauthorized access.	IT-approved, encrypted storage with access control (e.g., Microsoft OneDrive, SharePoint, Teams, or local network drives). Review file permissions periodically.
Hard Copy / Paper Storage	Follow Restricted Guidelines	Can be stored openly but should be organized and monitored.	Securely locked in filing cabinets or desks, accessible to relevant staff.
Laptops/Desktops	Follow Restricted Guidelines	Basic security (antivirus, firewall). There are no special restrictions on local storage.	Mandatory disk encryption. Strong authentication for access control. Auto-lock or log-off when unattended. Avoid local storage; transfer to secure network cloud storage promptly. Only organization-issued devices are permitted.
Printers & Printed Materials	Follow Restricted Guidelines	Dispose of unneeded prints securely.	Verify printer location; collect prints immediately. Avoid home printers for sensitive materials. Use approved

			shredders or bins for disposal. Use secure printing options where available. Printed materials should contain one of Rhode Island College's classification categories in the document footer on every page to inform readers of Rhode Island College's classification and treatment of this information. Alternatively, classification categories may be indicated on large amounts of printed data as part of a group, for example a cover page or envelope indicating all documents contained within are 'Restricted'. The exception for labeling is with marketing material since marketing material is primarily developed for public release.
Smartphones	Follow Restricted Guidelines	Encryption and strong authentication recommended. Use approved apps for data access.	Full device encryption. Strong PIN/biometric authentication. Secure container apps for restricted data. Remote wipe capabilities. Personal devices may be used with approved apps.
Text Messaging	Follow Restricted Guidelines.	Standard practices; maintain professionalism.	Transmitting restricted information is prohibited.
USB/External Drives	Follow Restricted Guidelines	Standard security practices; use for non-sensitive information recommended.	Use is restricted to encrypted, organization-provided USB drives. Personal devices are prohibited.
Video	Follow	Non-sensitive meetings	Secure, encrypted platforms

Conferencing	Restricted Guidelines	can use publicly available platforms.	(MS Teams, Zoom). Verify identities; limit sensitive information sharing. Information displayed or viewed (e.g., documents, presentations, etc.) must be labeled with its classification as part of the display.
Voicemail	Follow Restricted Guidelines	Basic security practices. Encourage clear and professional messages.	Secure access with PIN or password. Review and delete unneeded voicemails regularly. Prohibit forwarding/sharing outside authorized group. Delete immediately when no longer needed. Avoid requesting and leaving restricted information in voicemails.

ACCESS

For comprehensive details on our access control procedures, including protocols for granting, modifying, and revoking access to information assets based on roles and responsibilities, please refer to our Access Control Procedure document. This resource provides in-depth guidance on ensuring secure and authorized access, aligning with our commitment to protecting sensitive information. See [Link to Access Control Procedure] Will be posted August 2025

RETENTION AND DESTRUCTION

For detailed information on our data retention policies, which outline the duration for retaining various types of information and the proper methods for their secure disposal or archiving, please consult the following, which are essential for understanding how long information should be kept and the procedures for safely disposing of it once its retention period expires.

See [Link to Retention Schedule] Will be posted August 2025
See [Link to Destruction Procedures] Will be posted August 2025

CONTACT INFORMATION

AVP/CIO Information Technology Services
(401) 456-8200
avpis@ric.edu

REVISION HISTORY			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	3/24/2025	Initial Approval & Publication	[CIO]

Appendix A – Information Owners

The following table describes organization owners who have collectively classified information based on Record types.

Record Type	Information Owners
Directory Data	Legal, Risk Management, HR, Registrar
Financial, Sales, and Marketing	Finance / Marketing / Communications, Investment Team
Compliance & Legal Data	Legal, Risk Management, Audit
Personal Data (Student or Employee)	Registrar, Bursar, Advancement, HR
Student Performance Data	Registrar
HR Data	HR
Physical	Facilities / Campus Safety
Networking & Infrastructure Data	ITS

Appendix B – Data Types, Details

Appendix B categorizes various record types and their associated fields into three classification levels: Public, Internal, and Restricted. Please consider these tables when classifying information.

Public:

Type of Record	Field
Directory Data	First & Last Name
Directory Data	Organization Email Address
Directory Data	Department of Assignment (Including Office Telephone/Fax Number and Office Address)
Financial, Sales and Marketing Data	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)
Financial, Sales and Marketing Data	News Releases
Compliance & Legal Data	Policies

Internal:

Type of Record	Field
Directory Data	Home Address and Phone/Fax Number
Student Performance Data	Education History or Credentials
Directory Data	Date of Hire
Directory Data	Date of Separation
Directory Data	Employment Status
Personal Data (Student or Employee)	Email Address (Personal)
Personal Data (Student or Employee)	Employer Identification Number (EIN)
Personal Data (Student or Employee)	Ethnicity
Personal Data (Student or Employee)	Consumers or Employees IP Address
Personal Data (Student or Employee)	Age
Personal Data (Student or Employee)	Gender
Personal Data (Student or Employee)	Birth Date
Personal Data (Student or Employee)	Disciplinary Records

Personal Data (Student or Employee)	Political Opinions
Personal Data (Student or Employee)	Religious or Philosophical Beliefs
Personal Data (Student or Employee)	Trade Union Data
Personal Data (Student or Employee)	Dependent or Beneficiary Data
HR Data	Compensation & Benefits Data
HR Data	Workers Compensation Claim Data
Financial, Sales and Marketing Data	Incentives or Bonuses (amounts or percentages)
Financial, Sales and Marketing Data	Stock Dividend Information
Financial, Sales and Marketing Data	Investment-Related Activity
Financial, Sales and Marketing Data	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)
Financial, Sales and Marketing Data	Debt Amount Information
Financial, Sales and Marketing Data	SEC Disclosure Information
Financial, Sales and Marketing Data	Corporate Tax Return Information
Financial, Sales and Marketing Data	Legal Billings
Financial, Sales and Marketing Data	Budget-Related Data
Financial, Sales and Marketing Data	Unannounced Merger and Acquisition Information
Financial, Sales and Marketing Data	Business Plan (including marketing strategy)
Financial, Sales and Marketing Data	Financial Data Related to Revenue Generation
Financial, Sales and Marketing Data	Marketing Promotions Development
Financial, Sales and Marketing Data	Annual Reports
Financial, Sales and Marketing Data	Donation Information
Compliance & Legal Data	Regulatory Compliance Data
Compliance & Legal Data	Policy & Training Attestations
Compliance & Legal Data	Subpoena
Compliance & Legal Data	Titles
Compliance & Legal Data	Contracts
Physical	Non-Public Building Plans

Physical	Information about Physical Plants
Physical	Information About Alarm & Emergency Systems
Student Performance Data	Attendance Records
Student Performance Data	Grades
Student Performance Data	Test Scores
Student Performance Data	Course Information
Networking & Infrastructure Data	Service Provider Account Numbers
Personal Data (Student or Employee)	Labor history
Personal Data (Student or Employee)	Pictures/Photographs
Directory Data	Height and Weight

RESTRICTED:

Type of Record	Field
Compliance & Legal Data	Regulatory and Legal Filings
Compliance & Legal Data	Safety Incident Reports
Compliance & Legal Data	Investigation Reports
Compliance & Legal Data	Sexual Assault Reports
Personal Data (Student or Employee)	Tax Information
Personal Data (Student or Employee)	Government-Issued Identification (e.g., passport, permanent resident card, etc.)
Personal Data (Student or Employee)	Social Security Number (SSN)
Personal Data (Student or Employee)	Driver’s License (DL) Number
Personal Data (Student or Employee)	Payment Card Number (credit or debit)
Personal Data (Student or Employee)	Medical Condition or Diagnosis
Personal Data (Student or Employee)	Genetic Data
Personal Data (Student or Employee)	Biometric Data (retina, fingerprint, voice print)
Financial, Sales and Marketing Data	Electronic Payment Information (Wire Payment / ACH)
Financial, Sales and Marketing Data	Paychecks

Financial, Sales and Marketing Data	Bank Account Information
Networking & Infrastructure Data	Internal IP Addresses
Networking & Infrastructure Data	Username & Password Pairs
Networking & Infrastructure Data	Public Key Infrastructure (PKI) Cryptographic Keys (Public and Internal)
Networking & Infrastructure Data	Hardware or Software Tokens (multifactor authentication)
Networking & Infrastructure Data	System Configuration Settings
Networking & Infrastructure Data	Privileged Account Usernames
Student Performance Data Networking & Infrastructure Data	FAFSA Data Source Code