Rock Valley College

Institutional Data

RVC Administrative Procedure (2:30.060)

Purpose

Institutional data is information that supports the mission and operation of Rock Valley College (RVC). It is a vital asset and considered essential to the College. The confidentiality, integrity and availability of institutional data must be ensured to comply with legal, regulatory, and administrative requirements.

Scope

All electronic information that constitutes an official record, a record under any data privacy statute, or has institutional value, shall be managed responsibly with regard to data access, backup, and disposal. This Procedure describes the requirements for proper management of institutional data records.

Classification of Institutional Data

The overall sensitivity of institutional data encompasses not only its confidentiality, but also its integrity and availability. Many confidentiality obligations exist, such as those required for personal information and to meet contractual or regulatory requirements. Integrity, or trustworthiness, of institutional data must also be considered and aligned with institutional risk; that is, the impact on the institution should the data not be accurate. Availability relates to the impact on the institution's ability to function if the institutional data is not reliably accessible to authorized users. Four levels of sensitivity apply to institutional data:

Classification Level	Description	Examples
Critical	Inappropriate handling or disclosure of this data could cause severe harm to individuals and/or the College, including exposure to criminal and civil penalties, identify theft, personal financial loss, or invasion of privacy. Only selective access (on a need-to-know basis) may be granted.	Social Security Number, Credit Card and Payment Information, Driver's License Number

	It has the most stringent legal or regulatory requirements and requires the most prescriptive security controls.	
Restricted	Disclosure could cause significant harm to individuals and/or the College, including exposure to civil liability. Only selective access (on a need-to-know basis) may be granted. Usually subject to legal and regulatory requirements due to data that are individually identifiable, highly sensitive and/or confidential.	Personal Identifiable Information (PII) or Personal Health Information (PHI) - Financial aid data, student transcripts, workers compensation cases, payroll, Family Medical Leave Requests.
Internal	Disclosure can cause limited harm to individuals and the College with some risk of civil liability. Data may be accessed by eligible employees and designated appointees of the College for purpose of College business. Access restrictions should be applied accordingly.	Financial reports, department memos, committee meeting minutes
Public	Encompasses information for which disclosure poses little to no risk to individuals or the College. Few restrictions are placed on this data, as it is generally releasable to a member of the public upon request, or is published. Anyone regardless of institutional affiliation can access without limitation.	College and department websites, news releases, information subject to open records requests (email, financial, etc)

Rock Valley College

Access to Institutional Data – Privacy Rules

Authorization to access institutional data varies according to the need for care and caution in handling. For each classification, data handling requirements are defined to appropriately safeguard the information.

1. Authorization to access restricted and critical institutional data is approved by the Department of Information Technology and/or Data Steward (as defined in the Information Security Administrative Procedure), and is typically made in conjunction with the requestor's department head, supervisor, or other authority. Restricted and critical institutional data shall not be shared with individuals or departments, unless needed for that individual or department's purpose or business.

2. Where access to non-public institutional data has been authorized, use of such data shall be limited to the purpose for which access was granted.

3. Data Stewards and the Department of Information Technology must ensure that appropriate security practices, consistent with the data handling requirements in this Procedure, are used to protect institutional data. These requirements also apply to copies of the data.

4. Faculty and staff must affirmatively accept the College's Institutional Data Confidentiality Agreement on an annual basis as a prerequisite for obtaining access to non-public data. This document will be stored in the individual's personnel file. The College's Institutional Data Confidentiality Agreement shall be prepared, maintained, and updated by the COO, legal counsel, and the Department of Information Technology. The Institutional Data Confidentiality Agreement will be reflective of the data privacy obligations imposed by applicable statutes and in line with reasonable standards and practices.

5. Legal counsel must review external data sharing agreements to ensure appropriate enforcement of confidentiality.

Institutional Data Storage

Securing informational data is a critical aspect of data storage. Critical and restricted information contains information that if improperly disclosed could cause significant harm to individuals and/or the College, including exposure to civil liability.

Storage of this information is important, so any data deemed critical or restricted will be stored in a way that uses data encryption to further protect the data from unauthorized attempts to access it and that is a customary storage method for this type of data.

Any items that contain critical or restricted information transmitted utilizing RVC email system shall utilize the data encryption features of the email system.

Institutional Data Backup

All institutional data must be copied onto a secure storage media on a regular basis (i.e., backed up), for disaster recovery and business continuity purposes. This section outlines the minimum requirements for the creation and retention of backups. Special backup needs that exceed these minimum requirements should be implemented on an individual, as-needed basis and in consultation with the Department of Information Technology.

Data backup solutions by the Department of Information Technology are provided in order to meet or exceed minimum backup requirements for typical applications, however, Data Custodians must verify that backups meet the requirements of the data collections for which they are responsible. Services contracted from an outside vendor should be assessed to determine responsibility for backups, and ability to meet RVC's requirements.

Specific files on faculty and academic staff computers are backed up continuously, and stored encrypted. Versions of backed up files are retained for a rolling window of one year or as determined by the Department of Information Technology, and in compliance with applicable law.

The Department of Information Technology does not systematically back up student computers. However, it offers assistance to students to help them back up data to secure cloud storage, academic servers, and devices such as removable hard drives.

Federal and state regulations pertaining to the long-term retention of information (e.g., financial records, communications, etc.) must be met using retention policies as identified in the Records Retention Board Policy. Long-term archive requirements are beyond the scope of this procedure.

General Requirements

The Department of Information Technology, Data Custodians and Stewards will document backup and recovery procedures for each collection of institutional data that they maintain, which address:

1. Individuals responsible for performing backup and recovery operations.
2. Individuals to be notified in the event recovery operations are required.

3. Locations of backups, including requirements for off-site storage.
4. Rules governing who may access backups.
5. Backup and retention schedules.
6. Special requirements (e.g. data encryption, unique hardware, external regulations, etc.)
7. Step by step instructions on how to perform backup and recovery functions.

Equipment Disposal

Digital storage devices that contain licensed software programs and/or institutional data must be reliably erased and/or destroyed before the device is transferred out of the College's control or erased before being transferred from one department or individual to another. This does not preclude the use of physical media intended specifically for the purpose of data transfer.

All computers and digital storage devices including, but not limited to desktop workstation, laptop, server, notebook, handheld computer, and hard drives; and all external data storage devices such as disks, SANs, optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes), and non-volatile electronic media (e.g., memory sticks), are covered under these requirements for disposal.

Enforcement

Employees believed to be in violation will be referred to employee disciplinary procedures consistent with applicable College policies and contractual obligations. All other presumed violators will be handled on a case-by-case basis.

All requests for clarifications or interpretations of this procedure should be directed to the Vice President of Operations/COO.

Implemented: March 2023