Information Security

RVC Administrative Procedure (2:30.060)

Purpose

Information assets of the Rock Valley College (RVC), in all their forms and throughout their life cycle, will be protected through information management policies and actions that meet applicable federal, state, regulatory, or contractual requirements and support RVC's mission, vision, and values. The purpose of this policy is to identify and disseminate the College's framework and principles that guide institutional actions and operations in generating, protecting, and sharing institutional data.

Scope

This Procedure governs management of devices, resources, and user access to the College's owned equipment and institutional data. These information assets are classified within four sensitivity levels: public, internal, restricted, and critical, as set forth in the Institutional Data Procedure. All sensitivity levels other than "public" may be described collectively as "non-public" data. Each faculty, staff, student, contractor, or affiliate of the College with access to institutional data is subject to and has responsibilities under this Procedure.

General Guidelines

1. RVC is committed to ensuring the security and confidentiality of institutional data is maintained at all times, and that institutional data is only accessed appropriately in compliance with applicable laws.
2. Users (as defined herein) are individually responsible for any breaches that occur as a direct result of non-compliance.
3. Access to non-public institutional data may only be granted to Authorized Users (as defined herein) on a need-to-know basis. The Data Steward (as defined herein) of any non-public institutional data must approve, and verify Authorized User access.
4. Users who access data for which they are not authorized and/or commit breaches of confidentiality may be subject to disciplinary action up to and including discharge, termination of contract/relationship, and/or liability to civil and criminal penalties in accordance with the College's disciplinary policies.
5. Authorized Users shall be provided training on the expectations, knowledge, and skills related to information security.
6. Authorized Users must maintain the confidentiality of all non-public institutional data even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.

7. Authorized Users are responsible for enforcing security controls whenever they place institutional data onto non-College-managed devices or services.
8. All Users' access to College-owned or managed digital and or physical assets will comply with applicable standards, controls, and regulations (e.g., PCI-DSS, FERPA, HIPAA, GDPR, etc.).

Roles and Responsibilities

Responsibility for RVC's Enterprise Information Security Program is delegated to the groups and individuals as defined below. Note that an individual may function within more than one role (e.g., a network security contact for one unit may be an authorized user of data within another unit).

College Level Roles:
Data Trustee
Executive Director of Information Technology

Unit Level Roles:
Data Steward
Network Security Contact
Data Custodian
Authorized User

College Level Responsibilities

Data Trustee

The enterprise vice-president or organization-level executive having policy-level responsibility and authoritative decision making for a particular set of information assets. This position is occupied by the Chief Operations Officer (COO) or designee. The Data Trustee will:

1. Establish and communicate standards for business use of information.
2. Assign administrative responsibility to Data Stewards.
3. Monitor compliance and periodically review violation reports in coordination with the Department of Information Technology.

Executive Director of Information Technology

The official responsible for directing implementation of the Enterprise Information Security Program. The Executive Director will:

1. Coordinate the development and maintenance of information security policies and standards.
2. Investigate security incidents and coordinate their resolution as defined in the Network Vulnerability Assessment and Incident Response Procedures.
3. Advise Data Stewards in classifying their data and recommend available controls as defined in the Institutional Data Procedure.

4. Implement and execute an information security awareness program.

Unit Level Role Responsibilities

Data Steward

The senior official within a college or departmental unit (or his/her designee), accountable for managing information assets. This position is an Executive Director, Dean, or Director. The Data Steward will:

1. Approve business use of information.
2. Identify Data Custodian(s) (see below) for each segment of information under his/her control.
3. Ensure implementation of policies, and documentation of process and procedures for guaranteeing availability of systems, including:
   - Risk assessment
   - Disaster recovery
   - Business Continuity
   - Software testing and revision controls
4. Determine appropriate classification of each segment of data as described in the document and classify said segment of data in accordance with the relevant backup and recovery procedures, as required in the Institutional Data Administrative Procedure and other applicable procedures.
5. Define departmental access roles and assign access for individuals based on their business need to know.
6. Ensure that all department/unit personnel with access to information assets are trained in relevant security and confidentiality policies and procedures.

Network Security Contact

The individual within a unit who acts as a liaison for timely and relevant information flow between central networking and IT (Information Technology) security personnel and the unit.

The Network Security Contact will:

1. Receive vulnerability reports for unit computer systems and disseminate such information to appropriate technical staff for resolution.
2. Receive network alerts, outage notifications, or other networking issues affecting the unit and disseminate such information to appropriate staff.
3. Coordinate unit response to computer security incidents.

Data Custodian

Functional or technical user that has operational responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms. The data custodian may or may not be IT staff.

The Data Custodian will:

1. Define and implement processes for assigning User access, revoking User access privileges, and setting file protection parameters.
2. Implement system protection, data protection and access controls conforming to the Institutional Data Administrative Procedure.
3. Define and implement procedures for backup and recovery of information.
4. Ensure processes are in place for the detection of security violations.
5. Monitor compliance with information security policy and standards.
6. Limit physical and logical access to information assets, including:
    - Equipment control (inventory and maintenance records), and physical security of equipment (e.g., HVAC, locks).
    - Authorization procedures prior to physical access to restricted areas, such as data centers, with sign-in or escort of visitors, as appropriate.
    - Implement a system for software change management and revision controls. Maintain appropriate internal audit, which records system activity such as logins, file accesses, and security incidents.
    - Maintain records of those granted physical access to restricted areas (e.g., key card access lists).
    - Some of the above requirements may be delegated to others, when hosting within an institutional data center or when in the cloud. The data custodian will take appropriate steps to monitor these delegated requirements.

Authorized User

Individuals granted access to information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include but are not limited to faculty and staff members, agents, trainees, students, vendors, volunteers, contractors, or other affiliates of RVC.

Authorized Users will:

1. Seek access to data only through established authorization and access control processes.
2. Access only that data for which they have a business need to know to carry out job responsibilities.
3. Act in a reasonable manner so that no other individual or third-party can access data which they would not otherwise have access to.
4. Disseminate data to others only when authorized by the Data Steward.
5. Report access privileges inappropriate to job duties to the Data Steward for correction.
6. Complete training in information security and confidentiality policies and procedures.

7. When required by Board policies or otherwise, acknowledge or sign annual confidentiality statements for access to restricted and critical data. This document will be stored in the individual’s personnel file.
8. Perform all responsibilities necessary to protect data when placing institutional data on personally owned or managed devices.

Information Assessment, Classification, and Access

Data Stewards will assess risks and threats to data for which they are responsible, and accordingly classify and oversee appropriate protection of institutional data as described in the Institutional Data Administrative Procedure.

Physical and electronic access to institutional data must be controlled. The level of control will depend on the classification of the data and the level of risk associated with loss or compromise of the information. Data handling requirements are outlined in the Institutional Data Administrative Procedure.

Procedures must be documented for the timely removal of access to systems, services, and accounts, including return of institutionally owned materials (e.g., keys, ID Cards), for employees, affiliates, and contractors.

External Data Sharing

All non-public data shared or placed outside RVC’s control are subject to College policies and procedures, as well as applicable laws, rules, and regulations. For example, Protected Health Information (PHI) will only be shared based on the Health Insurance Portability and Accountability Act (HIPAA) regulations.

Institutional data transmitted outside the organization requires additional safeguards. The security provisions employed will depend upon the identified risk and threats, regulatory requirements, and the technical mechanisms available.

1. The Data Steward is responsible for making decisions regarding appropriateness of external transmission and access to institutional data.
2. The Executive Director of Information Technology will review and approve technical security mechanisms and services for remote access and external transmission of non-public institutional data.
3. Critical or restricted data transmitted and exchanged over open networks such as the public Internet or outside of the College’s managed network must be encrypted and/or include strong authentication.

Data Disposal

Proper data disposal is essential to controlling sensitive data. Remove sensitive information on all media or devices leaving control of the department, as described in the Institutional Data Administrative Procedure and applicable laws, rules, and regulations.

Enforcement

Non-compliance shall be reported to the Vice-President of Operations/COO. 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