Rock Valley College

Security Awareness Training

RVC Administrative Procedure (2:30.060)

Purpose

This Procedure establishes the requirements to ensure Rock Valley College's systems and data are appropriately safeguarded. Our staff and faculty are the frontline to protecting the College's data assets and this Procedure will assist at providing consistent guidance and overall approach to security awareness.

Scope

Rock Valley College (RVC) provides Security Awareness Training for all faculty, staff, contractors and business partners. The training will address roles, responsibilities, management commitment, proper disposal of data storage media, coordination among organizational entities and compliance.

Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position.

Individuals may be assigned multiple roles, as long as, the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

The Executive Director of Information Technology is responsible the maintenance, care, and security of all data assets, whether or not such assets are in the Executive Director of Information Technology's personal custody or control, this includes, but is not limited to the following:

1. Risk Assessment – Facilitate periodic risk assessments of data assets handling methods.
2. Design – Design and amend the Security Awareness Training, as may be required from time to time.
3. Implementation – Facilitate training on a periodic basis based on the needs of RVC.
4. Monitor – Evaluate this Procedure regularly, and ensure that all administrators, staff, faculty, contractors, vendors, and business partners are in compliance with this Procedure.

Rock Valley College

Staff and Faculty

Administrators, staff, faculty, contractors, vendors, and business partners who use RVC systems will be required to:

1. Complete an annual online Security Awareness Training program every twelve (12) months. All newly hired employees are required to complete the Security Awareness Training course within the first 30 days from date of hire.
2. Complete any additional Security Awareness Training that may be required by all employees at other intervals when IT infrastructure environment changes.
3. Read the "Acceptable Use Administrative Procedure" at the time of initial hire and any modification to the Administrative Procedure when published.

Supervisors, Managers, Deans, and Directors are required to:

1. Ensure each employee under his/her supervision has attended and completed the Security Awareness Training and should include the training as a part of the employee's annual performance evaluation.
2. Submit a written notice to their superior confirming that all subordinate employees have completed the Security Awareness Training course. Subsequently, the head of the Department shall submit a written compliance notice to the Human Resources Director.
3. Ensure that RVC faculty, staff, contractors and business partners who manage, administer, operate, or design IT systems, receive additional role-based information security training approved by the Executive Director of Technology as deemed appropriate and that is commensurate with their level of expertise, role and responsibilities.

Human Resources and Department of Information Technology Management

1. Oversee RVC's Security Awareness and Training program, including development, implementation and testing.
2. Coordinate, monitor and track the completion of the Security Awareness Training for all RVC faculty, staff, contractors and business partners and report incomplete training to the respective senior executive, manager or accountable person.
3. Design the role-based training program and maintains records of training for entire program.

General Requirements

1. All RVC employees (permanent, temporary, contractual, faculty, and administrators) who use RVC information technology resources to conduct College business and to transmit sensitive data in the performance of their

jobs must take Security Awareness Training prior to using RVC systems, when required information systems change; and annually thereafter.

2. In an effort to educate RVC system users in understanding their responsibility in safeguarding systems and data, Security Awareness Training may include, but is not limited to, the following concepts:
    a. Procedures for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
    b. Prevention and detection of information security incidents, including those caused by malicious code;
    c. Proper disposal of data storage media;
    d. Proper use of encryption;
    e. Access controls, including creating and changing passwords and the need to keep them confidential;
    f. Acceptable Use Administrative Procedures
    g. Remote Access Administrative Procedures
    h. Phishing and Social Engineering;
3. Role specific training will be provided to the following specialized users (System Owners, Data Trustees, Data Stewards, Data Custodians, and the Department of Information Technology Security Administrators). Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. This training will also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to the College.

Enforcement

All requests for clarifications or interpretations of this procedure should be directed to the Vice President of Operations/COO who will work with the Executive Director of Technology and the Director of Human Resources.

Implemented: March 2023