Rock Valley College

Incident Response

RVC Administrative Procedure (2:30.060)

Purpose

Much of the data stored or transmitted via Rock Valley College's (RVC) systems, network, and resources is confidential. Unauthorized access to such data may constitute a violation of federal statutes such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and other laws designed to protect data privacy. A breach in data security that compromises personal information may put members of the RVC community at risk and/or expose the College to litigation or other data security remediation measures. Unauthorized access to other confidential data, though not usable for identity theft, may nonetheless have serious legal, financial, or reputational implications for the College. RVC's response to any cyber incident may minimize the harm to both the individuals and the College.

Scope

All devices attached to RVC's network may be subject to a cyber incident. In general, confidential data should not be accessed, copied, stored, downloaded, transmitted, or used. Attacks on RVC resources are violations of the Acceptable Use Procedure and may also be vandalism or other criminal behavior. Attacks on the College's resources will not be tolerated, and this Procedure provides a method for pursuing the resolution and follow-up for incidents.

Reporting information security incidents occurring on the College's systems and/or network to the appropriate authorities is a requirement of all persons affiliated with the College in any capacity, including staff, agents, vendors, students, faculty, contractors, and visitors.

Incident Response

The individual or entity responsible for support of the system or network that has been compromised or is under attack is in all cases expected to:

1. Report the incident to their leadership and to the Department of Information Technology immediately.
2. Take action at the direction of the Department of Information Technology to contain the problem, and block or prevent escalation of the attack, if possible.
3. Follow instructions communicated from the Department of Information Technology to facilitate investigation of the incident and preservation of evidence.

4. Implement recommendations from the Department of Information Technology to remediate the system, and repair resulting damage, if any.
5. Restore service to its former level, if possible.

The Department of Information Technology shall:

1. Identify potential ongoing exposure of data and take immediate steps to close holes.
2. Conduct preliminary forensic analysis and work with outside assisting agencies on an as needed basis.
3. Prepare inventory of data at risk and identify affected individuals whose data was potentially impacted.
4. Determine if exposed data was encrypted.
5. Identify security measures that were defeated.
6. Implement password changes and other security measures to prevent further data exposure.
7. Determine if exposed/corrupted data can be restored from backups, and execute any potential backups.
8. Communicate with Vice-President of Operations/COO to determine if any steps are statutorily required or required by another policy or procedure.

Internal Notifications

The Executive Director of Information Technology will report serious computer security breaches to the Vice-President of Operations/COO. The COO will report to the Cabinet and/or the General Counsel when, based on preliminary investigation, criminal activity has taken place and/or when the incident originated from within the RVC network or from College-owned equipment.

External Notifications

No later than seventy-two (72) hours after becoming aware of the cyber security incident, the COO, in consultation with the Cabinet and General Counsel, shall promptly notify the College's insurance provider of any incident where confidential information may have been compromised. The COO, after consultation with the Cabinet, General Counsel, and the College's insurance provider, contact any legal authorities as needed.

Public Notification of Breach

To determine whether public notification is required, the COO will consult with the Cabinet and General Counsel and others as appropriate. Departments may not perform public notification without COO approval.

Individual Notification of Breach

To determine whether individual notification of a breach is necessary, the COO will consider all relevant factors (such as legal or regulatory requirements, credible evidence the information was compromised and in a usable format, ability to reach the affected individuals, etc.).

If it is determined that a notification of breach to affected individuals is warranted, the following procedures will apply:

1. The notification will be drafted by the affected department and submitted to the COO and General Counsel for review and approval.
2. Written notice will be provided to the affected individuals based on legal or regulatory requirements, and may be sent via personal email or US Mail.

Incident Response Planning

The Department of Information Technology:

1. Maintains an internal, standardized incident response framework that includes protection, detection, analysis, containment, recovery, and user response activities, which may be amended from time to time.
2. Annually, at a minimum, tests the incident response framework and associated capabilities in order to determine the framework's effectiveness. The results of this testing are then used to improve the incident response framework.
3. Actively monitors and blocks specific countries or other entities involved in identified attacks or other malicious activities.

Enforcement

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

Implemented: March 2023