Rock Valley College

Network Vulnerability Assessment

RVC Administrative Procedure (2:30.060)

Purpose

Regular scanning of devices attached to the network to assess potential security vulnerabilities is a best practice for managing a dynamic computing environment. For critical enterprise systems or those dealing with sensitive data, additional testing methods to look deeper for more security vulnerabilities may be a requirement for compliance with laws, regulations, and/or policies.

This Procedure provides guidance in determining the proper response to a network security incident from within or outside Rock Valley College (RVC). The Procedure also documents where to report problems and how the College will involve leadership and legal representatives. It also documents the individuals designated for these responsibilities, and procedural details, which depend on the severity and source of the attack.

Scope

All devices attached to RVC's network are subject to security vulnerability scanning and/or penetration testing. Systems that are not properly managed can become a potential threat to the operational integrity of our systems and networks, and subsequently, any of the College's data assets. Other systems dealing with sensitive data may be submitted for penetration testing at the request of the Data Trustee (defined in the Institutional Data Administrative Procedure).

Penetration testing is a separate and distinctly different set of testing activities from vulnerability scanning. Its primary focus is the exploitation (not just observation or assessment) of security vulnerabilities and therefore, it may be disruptive of operations. Penetration testing is most beneficial when executed after an Assessment has been performed and the issues found by that Assessment have been remediated.

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.

Network Security Scanning and Assessment

Multiple levels and types of network security scanning are utilized by RVC and are managed as services offered by the Department of Information Technology:

1. Routine Scans – Low-level scans for basic service-tracking and vulnerability identification purposes will be conducted on all networks within the College's domain.
2. Ad Hoc Scans – Scans may be conducted by system administrators at any time, as frequently as necessary to maintain confidence in the security protections being employed. Any system identified in conjunction with a security incident, as well as any system undergoing an audit, may be subject to a network security scan without prior notification.
3. Penetration Test – All penetration testing of RVC systems must be arranged by the Data Trustee(s) and coordinated through the Department of Information Technology. Penetration testing is typically conducted over a period of several weeks, with regular feedback to the Data Trustee(s) if issues are identified.

The Department of Information Technology shall use its expertise and discretion to update and utilize scanning and assessment types that are in consistent with industry standards, and which are helpful to the College.

Vulnerability Remediation

Vulnerabilities that are identified during network vulnerability assessments will be communicated to system owners. The affected departments and units must work with the Department of Information Technology toward vulnerability remediation, mitigation, or implementing compensating controls to reduce risks identified in vulnerability assessments. The Department of Information Technology and the affected departments and units will work together to expeditiously patch and resolve the vulnerability.

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.

Enforcement

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

Implemented: March 2023