Rock Valley College

Firewall, Router, and Switch Administration

RVC Administrative Procedure (2:30.060)

Purpose

This Procedure documents the core principles for the configuration and maintenance of our firewall infrastructure. There are many components that make up the cyber-security defenses at Rock Valley College (RVC). However, at the core is the protection of the perimeter of our network from external attacks and intrusions using firewall and supporting network technologies.

Scope

This Procedure applies to RVC firewall installations and all RVC network infrastructure components. Accountable and responsible individuals are the Executive Director of Information Technology, IT (Information Technology) Service Desk support personnel, and Network and Infrastructure support management and staff.

Summary

Each connectivity path and service to and within the RVC network shall be managed and protected by firewalls, routers, and switches that are configured and administered according to defined and documented standard operating procedures. The Department of Information Technology shall oversee these systems and shall update these systems from time to time in line with industry standards and practices.

Changes to firewall hardware, software, or security rules shall be reviewed, approved, logged, and implemented using documented change control standard operating procedures.

This Administrative Procedure shall be subject to and superseded by applicable regulations and laws.

Standards

1. Every connectivity path and service shall be managed by RVC firewalls.
2. All externally initiated inbound traffic shall only be permitted into a firewall segmented demilitarized zone (DMZ) network. In all cases, this traffic shall be limited only to ports necessary for RVC's business requirements.

3. At least every six months, the Network and Infrastructure Manager and the Department of Information Technology shall ensure a thorough review occurs for each firewall rule set and record the results of the review.
4. Internal IP addresses shall be hidden utilizing Network Address Translation (NAT) or Port Address Translation (PAT).
5. Anti-spoofing technologies shall be configured on perimeter devices.
6. Outbound traffic from internal production systems shall be restricted to only required protocols and services.
7. On-premises enterprise databases shall be segmented from the larger RVC network.
8. Specially regulated services and information (e.g., HIPAA, PCI) shall be configured on dedicated, isolated network segments that conform to regulatory standards.
9. Internet and wireless access to the core RVC network shall be regulated using next generation firewalls.
10. Where VLANs are used for segmentation, appropriate network security principles (e.g., ACLs) shall be implemented.
11. Network hardware devices and operating systems shall be upgraded, patched, and maintained to manufacturer recommendations and standards.
12. RVC reserves the right to report security violations or compromises to the appropriate authorities, and shall do so in its discretion, and when it is required to do so by law. This may include reporting violations of Federal, State, and local laws and regulations governing computer and network use or required accreditation reporting.
13. RVC shall block access to and from any host which it deems a risk to the College, contains illegal material, material containing pornography, or any other inappropriate material in the sole and absolute discretion of the College.
14. Anyone who violates this policy may be held liable for damages to RVC assets, including but not limited to the loss of information, computer software and hardware, lost revenue due to disruption of normal business activities or system down time, and fines and judgments imposed as a direct result of the violation.
15. RVC reserves the right to deactivate any user's access rights (whether the user is suspected of a violation of this policy) when necessary to preserve the integrity of IT Resources.

Exceptions

Exceptions to this policy must be pre-approved in writing by the Vice President of Operations/COO.

Enforcement

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

Implemented: March 2023