Vulnerability Management Policy

ROWAN UNIVERSITY POLICY

Title: Vulnerability Management Policy
Subject: Information Security
Policy No: ISO:2019:02
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Director of Information Security and Associate Director of Security Operations
Date Adopted: 10/17/2019
Last Revision: 10/17/2019
Last Review: 10/17/2019

I. PURPOSE

Vulnerability management is the processes and technologies that an organization utilizes to identify, assess, and mitigate information technology (IT) vulnerabilities, weaknesses, or exposures in IT resources or processes that may lead to a security or business risk. This policy identifies Rowan University’s vulnerability management practice which includes the roles and responsibilities of personnel, the vulnerability management process and procedures followed, and the risk assessment and prioritization of vulnerabilities.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer, Director of Information Security and Associate Director of Security Operations shall ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to any information asset, product or service that requires processing, transmitting or storage of Rowan data or information.

IV. DEFINITIONS

Refer to Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

V. POLICY

1. Vulnerability management is a process by which the vulnerabilities identified through scanning are tracked, evaluated, prioritized and managed until the vulnerabilities are remediated or otherwise appropriately mitigated. Mitigating the vulnerabilities identified during scans ensures that appropriate actions are taken to reduce the potential that these vulnerabilities are exploited and thereby reduces the risk of compromise to the confidentiality, integrity and availability of Rowan University information assets. All Rowan University information assets must be identified, scanned, reviewed and remediated or mitigated per the requirements of the vulnerability management policy.
2. Information assets handling Rowan University data must run currently supported operating systems, be patched and maintained regularly unless an exception has been provided by the Information Security Office.

3. System Owners or Administrators responsible for systems connected to the University network are required to allocate or obtain resources to mitigate issues identified by the vulnerability scans that are not otherwise addressed by regular patching. System Owners or Administrators are required to review the results of vulnerability scans and evaluate, test and mitigate system and application vulnerabilities appropriately.
4. Vulnerability Assessment and Scanning Methodology
   a. Scanning Tools: Vulnerability scans must be conducted using scanning tools approved by the Information Security Office. Any approved scanning tool must be able to provide remediation suggestions and be able to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the affected system.
   b. Scanning Schedule: Rowan University utilizes automated tools to scan systems, computing and network devices, web applications and application code. The results of these scans help inform management, system owners and system administrators of known vulnerabilities. All vulnerability scans must be scheduled and performed on a recurring basis per the scan schedule in **Table 1**.
   c. Agentless or Agent Based Scans: Authenticated scans using an agentless scan with credentials where applicable or an agent based scan without credentials must be used for all assets. This setup will be guided based on the recommended configuration from the system and scanning tool vendor. If the authenticated scan fails, the vulnerability scanning solution must default to a non-authenticated scan.
   d. Scan Types: New information assets must be scanned immediately upon being placed into the target implementation environment with the appropriate scan type for the asset. The appropriate type of plugin or checks used during the vulnerability scan for a given target depends on the target type (i.e., hardware, software, source code) and the target's location (i.e., internal or external to the Rowan University network. **Table 2** lists the types of vulnerability scans required by this policy.
   e. Risk Rating
      i. The risk that vulnerabilities pose to systems and applications is based on the likelihood of a vulnerability being exploited and the impact if the confidentiality, integrity or availability of the Rowan University information asset were to be compromised. The likelihood of a vulnerability being exploited is increased in direct relation to the system's or application's accessibility from other systems.
      ii. The impact to Rowan University's information assets is based on the asset's Information Classification as described in **Table 7** and the Impact (i.e., critical, high, medium or low). If the confidentiality, integrity or availability is compromised it must be considered and the highest individual impact rating for confidentiality, integrity or availability utilized within **Table 3**.
5. Vulnerability Remediation and Mitigation
   a. All vulnerabilities found during scans must be addressed as per the remediation information in **Table 6**. Any system or application deployed to its target implementation environment with un-remediated vulnerabilities must have a formal remediation or mitigation plan and the documented approval of the Information Security Office.
   b. Any infrastructure vulnerability that is determined to be a false positive or insignificant risk must be reported to the Security Operations team to complete verification and due diligence with the information asset and scanning tool. The Security Operations team is responsible for completing the analysis and reviewing the results with the Information Security Office.
   c. The Security Operations is responsible for performing the validation and testing to verify that remediation has been completed and if required, setting up additional scans to validate.
   d. The System Owner and/or System Administrator must provide notification for any outstanding vulnerabilities that are unable to be remediated in a timely manner. Any system or application deployed to its target implementation environment with un-remediated vulnerabilities must have a formal remediation plan or compensating controls that is approved and monitored by the Information Security Office.
   e. The Information Security Office will be notified of any un-remediated vulnerabilities not addressed in the timeframes prescribed in this policy, so that the process for assessing the residual risk can be followed.
6. Risk Assessment and Acceptance

   a. If a system vulnerability cannot be remediated or mitigated, the System Owner must complete a Risk Acceptance request and submit to the Information Security Office for review. The Risk Acceptance request must describe the business justification, remediation work plan and compensating controls that were attempted to remediate or mitigate a system vulnerability or the system limitations that prevent remediation or mitigation of the vulnerability.
   b. Risk Acceptance requests that have met the criteria for review based on the risk assessment process will be presented by the Director of Information Security to the Incident Board. The board must review the Risk Acceptance request and determine if the university should accept the risk of a system vulnerability that is unable to be remediated or if the system vulnerability is deemed an unacceptable risk and its activity suspended until proper controls are in place.
7. Exceptions
   a. No information assets are exempt from the Vulnerability Management program. However, a system owner can request an exception (or exclusion) for an information asset from vulnerability assessments or a modified scanning frequency by contacting the Information Security Office.
   b. The Information Security Office will review all requests to ensure the appropriate vulnerability assessments methodology or compensating controls are present to protect Rowan University's network prior to approving an exception.
8. Monitoring
   a. The Information Security Office is responsible for conducting annual reviews of:
      i. Accepted Risks to ensure applicability to the environment and maintaining the risk acceptance for an information asset.
      ii. Vulnerability exceptions to ensure the exception is still warranted
      iii. Application Classification and Ownership Recertification to ensure that information asset ownership, information classification and other details about an information asset are accurate.

VI. POLICY COMPLIANCE

Information Security may escalate issues through layers of management based on the severity of the non-compliance or the number of times non-compliance has been detected. Unless a previous exception has been approved by the Information Security Office, related services, access or network connectivity for the offending information asset will be suspended until the Information Security Office has received a written summary of corrective actions, signed by the individual, their manager, and if necessary the appropriate Dean or VP for the department.

	Individual System Owner Notification	**Supervisor, Dean and VP Notification**	**System Suspended**
First Incident	Yes		
Second Incident	Yes	Yes	
Third Incident	Yes	Yes	Yes

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer