

Vulnerability Management Policy

# Overview/Purpose

Vulnerability management is an essential component of any information security program.  The process of vulnerability assessment is vital to effective vulnerability management.

# Scope

Vulnerability assessment consists of scanning to identify networked assets, determining potential vulnerabilities, and assessment of potential vulnerabilities. Remediation of the vulnerabilities is another facet of vulnerability management.

# Policy

## Vulnerability Reports

All identified vulnerabilities will be assigned a risk ranking from Low to High based on industry best practices such as the CVSS base score. The results of vulnerability reviews will be documented on the vulnerability report. Mitigation actions are prioritize based on vulnerability ranking.

## Vulnerability Scans Frequency

As part of the PCI DSS Compliance requirements, **<Utility Name>** will run internal and external network vulnerability scans at least quarterly, and after any significant change to networks and systems (new application installation, new firewall or router installation, network equipment replacement, new server or workstation installation).

Quarterly internal vulnerability scans must be performed by the **<Utility Name>** IT department or a 3rd party vendor. The scan process must include rescans, to be repeated until passing results obtained, or all High vulnerabilities as defined in PCI DSS Requirements 6.2 are resolved.

Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by the PCI Security Standards Council (SSC). Scans conducted after network changes may be performed by **<Utility Name>** IT department. The scan process should include re-scans until passing results are obtained.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adopted from <https://www.sans.edu/student-files/projects/vulnerability-assessment-policy.pdf>
* PCI DSS Requirements   
  (<https://www.pcisecuritystandards.org/document_library>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **IT Department** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |