**Vulnerability Management Standard**

Classification: **Confidential**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Valid from | Next Review | Authorized by | Date |
| 1.0 | 15/3/25 | 15/9/25 | CISO | 20/3/25 |

# Overview

* Vulnerability Management (VM) serves as the company's mechanism to ensure the security of IT assets.
* It involves identifying technical weaknesses within IT environments and assessing these vulnerabilities.
* The remediation of such weaknesses is conducted systematically and in a prioritized and timely manner, in collaboration with IT teams.

# Purpose

* To define the requirements for the identification, assessment/classification, and remediation of technical vulnerabilities within <Company Name>.
* To establish the organizational stakeholders accountable for ensuring compliance with this standard.

# Scope

* This standard applies to all company’s IT systems and applications whether on-premises or in the cloud.
* Third-party systems connected to the company’s networks.
* Any asset that stores, processes, or transmits sensitive or regulated data.

# Roles and Responsibilities

* **Security Operations Management Team**:
  + Responsible for conducting vulnerability scans and penetration testing, assessing vulnerabilities, and guiding remediation teams in their efforts.
* **IT Service Teams**:
  + Tasked with remediating identified technical vulnerabilities in accordance with the standard.
* **Workplace Management**:
  + Accountable for communicating patching and upgrade schedules.
* **CISO (Chief Information Security Officer)**:
  + Ensures the availability of appropriate resources, specification, implementation, and compliance with security controls and baselines for IT assets.

# Standard

**5.1 General Requirements**

* All systems and applications are subject to vulnerability management practices, which include:
  + Scanning for technical vulnerabilities using the company’s approved scanning tools.
  + Reporting vulnerabilities identified during the scanning process.
  + Prioritizing and assessing vulnerabilities.
  + Implementing remediation measures, including patching, reconfiguration, or other methods as deemed necessary by qualified personnel.
  + Validating remediated vulnerabilities through an agreed-upon reporting format.

**5.2 Vulnerability Scanning**

* IT assets within scope must undergo regular scanning as follows:
  + Routinely, all deployed and operational assets should be scanned at least once per month (weekly for critical assets).
  + Ad hoc scans as specified by the Security Operations Management Team.
  + Scanning of new assets prior to deployment in operational environments.
* The type of scanning (authenticated or non-authenticated) is determined by the Security Operations Management Team.
* Scanning technology must be updated and maintained with latest vulnerability management information (Intelligence and Signatures)

**5.3 Vulnerability Assessment**

* Reports generated from vulnerability scans must be analysed within a maximum of two working days by qualified personnel.
* Vulnerabilities must be classified according to their severity using the CVSS (Common Vulnerability Scoring System):

| **Vulnerability Criticality** | **Vulnerability Score** |
| --- | --- |
| Critical | 9–10 |
| High | 7–8.9 |
| Moderate | 4–6.9 |
| Low | 0.1–3.9 |

* The analysis must consider the company’s existing security controls, adjusting criticality accordingly.
* False positives must be identified and excluded from the final report.

**5.4 Vulnerability Remediation**

* Documented vulnerabilities must be communicated to the staff responsible for IT asset operations and maintenance within a maximum of two working days.
* Remediation actions must adhere to the following resolution timeframes, starting from the time of communication:

| **Vulnerability Criticality** | **Remediation Resolution Requirements** |
| --- | --- |
| Critical | 1 working day (5) |
| High | 2 working days (20) |
| Moderate | 5 working days (60) |
| Low | 10 working days (120) |

**5.5 Penetration Testing**

* Conduct comprehensive external penetration testing annually, facilitated by an independent and qualified third-party provider
* Perform internal penetration testing biannually, or immediately following substantial changes to the infrastructure
* Ensure the scope of all tests includes network infrastructure, cloud environments, and web applications to provide thorough coverage
* Document all findings in detail and integrate them seamlessly into the organization's vulnerability management and remediation workflow

# Standards of Compliance

**6.1 Compliance Measurement**

* The Security Operations Management Team will verify adherence to this standard through audits of scan and remediation reports.
* KPIs tracked include:
* Percentage of critical vulnerabilities resolved within agreed-upon timelines
* Percentage of assets successfully scanned as per scheduled framework
* Number of overdue critical and high-severity vulnerabilities outstanding
* Quarterly compliance performance reports delivered to Risk Committee

**6.2 Exceptions**

* Any exceptions to this standard must be formally requested and approved by the Security Operations Management Team, in accordance with the exception request process.

**6.3 Reporting Requirements**

* Vulnerability scan reports are to be disseminated to the relevant teams within 24 hours of scan completion
* Comprehensive monthly vulnerability management reports, summarizing key findings, remediation progress, and unresolved risks, shall be presented to senior management

**6.4 Non-Compliance**

* Non-compliance with this standard may result in sanctions or disciplinary action by executive management, as outlined in the HR policy.

## Related Standards, Policies, and Procedures

* IT Security Policy
* IT Patching Standard
* IT Configuration Baselines
* Vulnerability Management Procedure
* NVD Website
* Additional Related Resources

# 8. Definition of Terms

|  |  |
| --- | --- |
| Term | Meaning |
|  |  |
| VM | Vulnerability Management: The process of identifying, assessing, and remediating vulnerabilities in IT systems and applications. |
| Vulnerability Management Information | Data related to vulnerabilities obtained from sources such as the National Vulnerability Database (NVD), along with threat intelligence insights. |
| NVD | National Vulnerability Database: A repository of standardized vulnerability information that is maintained by the U.S. National Institute of Standards and Technology (NIST). |
| CVSS | Common Vulnerability Scoring System: A framework used to evaluate and categorize the severity of security vulnerabilities. |
| Threat Intelligence | Contextual information about current and emerging threats, gathered to help prioritize and mitigate vulnerabilities. |
| Authenticated Scan | Vulnerability scanning that requires credentials to access systems, ensuring a more thorough assessment. |
| Non-Authenticated Scan | Vulnerability scanning performed without credentials, providing an external view of the system's security posture. |
| False Positive | A reported vulnerability that is not actually exploitable or relevant, requiring validation and exclusion from final reports. |

# 9. Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| 22/03/2025 | Cybersecurity Course Participants | Creation |
|  |  |  |