[Company Logo]

VULNERABILITY MANAGEMENT POLICY

The purpose of Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

Document Owner
Head of IT/Security

[Company Logo]	**CONTROLLED DOCUMENT** **Vulnerability Management Policy**	Document: Vulnerability Management Policy Developed by: Reviewed by: Approved by:

Vulnerability Management Policy

For

[Company Name]

Version: 1.0
Date: 01/01/0000
Next Review Date :

Note: Verify with the Policy Owner if this is the correct and latest version before use.

Revision History

Rev. #	Date	Modification Details	Page#	Suggested By	Reviewed By	Approved By
1.0		First Draft	NA			

Table of Contents

Purpose

The purpose of the Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them. Security vulnerabilities identified through scans or identified by vendors must be remediated/controlled as described below.

Scope

This policy applies to:

- All IT assets owned/operated by [Company Name], including:
    - Network infrastructure
    - Servers (physical/virtual)
    - End-user devices
    - Cloud environments
    - Applications (internal/third-party)
- All employees, contractors, and vendors with access to company systems
- Processes for identifying, assessing, prioritizing, and remediating vulnerabilities

Objective

The objective of the Vulnerability Management Policy is to:

1. Vulnerability management's main objectives are to scan, investigate, analyze, and report the details of risk or security vulnerabilities with mitigating methods and strategies.
2. Vulnerability management is the continuous process to address and remediate security vulnerabilities to avoid cyberattacks or exploitations.

Responsibility & Accountability

1. IT Security Team:
    - Conduct regular vulnerability scans (weekly/monthly)
    - Prioritize risks based on CVSS scores and business impact
    - Track remediation and verify fixes within SLA timeframes
2. System Owners:
    - Patch systems according to criticality tiers:
        - Critical (≤72 hours)
        - High (≤2 weeks)
        - Medium (≤30 days)
    - Document exceptions with risk acceptance forms
3. Employees:
    - Report unusual system behaviour immediately
    - Install approved updates on personal devices accessing company data
3. Executive Leadership:
    - Approve resources for vulnerability management tools
    - Review quarterly risk reports

Non-Compliance

Any Non-Compliance with this Vulnerability Management Policy will be dealt with Disciplinary Action as decided by the organization and respective authorities.

Exceptions

Not Applicable.

Policy Statement

- **Vulnerability and Patch Management Plan:**

1. The plan must include supporting activities such as training and reporting metrics for effective implementation of the vulnerability and patch management program.
2. The plan must include roles and responsibilities of teams/roles for accomplishing all the activities of the vulnerability management program in a timely and effective manner.
3. All Information Resources must be scanned regularly to identify missing updates.
4. All missing software updates must be evaluated according to the risk they pose to
5. Software updates and configuration changes applied to Information Resources must be tested before widespread implementation and must be implemented under the (District/Organization) Change Control Policy.
6. Verification of successful software update deployment will be conducted within a reasonable period as defined in the (District/Organization) Patch and Vulnerability Standard.

- **Vulnerability Scanning:**

1. Vulnerability scans of the internal and external network must be conducted at least quarterly or after any significant change to the network.
2. Failed vulnerability scan results rated at Critical or High will be remediated and re-scanned until all Critical and High risks are resolved.
3. Upon identification of new vulnerability issues, configuration standards will be updated accordingly.
4. The annual penetration test must be commissioned as required, using external qualified specialists as part of a carefully planned exercise, The plan must address the scope of the assessment, the methods to use, and the operational requirements, in order to provide the most accurate and relevant information about current vulnerabilities, without affecting the operation of the organization.

- **Endpoint Protection:**

1. The endpoint protection software must not be altered, bypassed, or disabled.
2. Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
3. All files received over networks or from any external storage device must be scanned for malware before use.

- **Inform System Administrators and System Owners:**

1. Application and system owners are responsible for the assessment and remediation of IT Resources under their management or supervision.
2. Application and system owners must have a written and auditable procedure addressing remediation steps.
3. All the vulnerabilities and respective remediation information must be communicated to all the affected users, including system administrators, system owners, and end users.

- **Penetration Testing:**

1. Penetration testing of the internal network, external network, and hosted applications must be conducted at least annually or after any significant changes to the environment.
2. Any exploitable vulnerabilities found during a penetration test will be corrected and re-tested to verify that the vulnerability was corrected.

Conclusion

Proactive vulnerability management is essential to protect [Company Name] from evolving cyber threats.

- This policy ensures:
  Systematic identification of weaknesses
  Timely remediation aligned with risk levels
  Clear accountability across teams

Annual reviews will keep our approach effective against new attack vectors.

<<< End of Document >>>