1. Policy Overview

The vulnerability management policy establishes a formal process that enables departments to protect **[Company name]**'s employees, assets, regulatory compliance, and the confidentiality, integrity, and availability (CIA) of company systems. This is achieved through the timely identification, evaluation, prioritization, and remediation of security vulnerabilities.

---

2. Scope

This policy applies to all assets, endpoints, networks, and associated applications that are owned, operated, or managed by **[Company name]**.

---

3. Roles & Responsibilities

- **Chief Information Security Officer (CISO):** Provides oversight of the vulnerability management program and ensures compliance with this policy.
- **Chief Information Officer (CIO):** Ensures vulnerability management practices are integrated into **[Company name]**'s overall IT strategy.
- **Department Heads:** Ensure compliance with this policy within their respective departments.
- **Security Operations:** Responsible for discovering, identifying, and validating vulnerabilities.
- **Risk/GRC:** Responsible for assessing risk, prioritizing vulnerabilities, and reporting vulnerability status.
- **IT Operations:** Responsible for remediating identified vulnerabilities.

---

4. Vulnerability Scan Schedule

The Security Operations Center (SOC) will oversee vulnerability scanning activities on the following basis:

- **Monthly:** On the first day of each month, a comprehensive authenticated scan will be conducted on all endpoints to identify vulnerabilities and configuration weaknesses.

- **Weekly:** Every Sunday (excluding the week of the monthly scan), a limited unauthenticated scan will be conducted to identify critical or high-risk exposures.

---

5. Vulnerability Classification and Severity

Vulnerabilities shall be classified based on the Common Vulnerability Scoring System (CVSS) and aligned with **[Company name]**'s current business objectives and risk tolerance.

- **Critical (CVSS 8.0–10.0):** Remediate or mitigate within 72 hours

- **High (CVSS 6.5–7.9):** Remediate or mitigate within 7 days

- **Medium (CVSS 4.0–6.4):** Remediate or mitigate within 30 days

- **Low (CVSS 0–3.9):** Remediate or mitigate within 120 days

---

6. Maintenance Plans

- **Emergency Patching:** Critical-level vulnerabilities must be patched within 72 hours whenever feasible.

- **Emergency Mitigation:** Temporary protective measures (e.g., access restrictions, firewall rules) must be implemented within 72 hours when immediate patching is not possible, allowing time for permanent remediation.

- **Routine Patching:** Security patches and updates shall be applied on a monthly basis as part of standard maintenance activities.

---

7. Exceptions & Risk Acceptance

In the event that a vulnerability cannot be remediated within the defined timeframes, the following must be documented:

- A justification explaining why remediation could not be completed within the required timeframe

- An estimated timeline for remediation or permanent mitigation

The duration of the exception must be approved by the CISO based on vulnerability severity and business impact. The exception must also be formally signed off by the designated risk owner and the CIO. At the conclusion of the approved timeframe, the exception shall be reviewed to determine whether further action is required.

---

8. Verification & Validation

All remediation efforts must be verified and validated through appropriate testing. Verification activities shall include a re-scan of the affected environment and manual validation of implemented changes to confirm that the vulnerability has been successfully remediated or mitigated.

---

9. Reporting and Metrics

Each identified vulnerability shall be documented in a written report that includes, at minimum:

- **Vulnerability description:**
  A brief summary of the vulnerability, including CVE information where applicable

- **Severity classification:**
  CVSS score and assigned severity level (Critical, High, Medium, Low)

- **Affected assets:**
  Systems, endpoints, applications, or network components impacted

- **Discovery details:**
  Date of discovery and method of detection (e.g., automated scan, manual review,

external report)

- **Risk assessment:**
  Potential impact on confidentiality, integrity, and availability

- **Remediation actions taken:**
  Description of patches, configuration changes, or compensating controls applied

- **Timeline metrics:**
    - Date identified
    - Date remediation began
    - Date remediation completed
    - Total time to remediate

- **Verification status:**
  Confirmation of remediation through re-scan and/or manual validation

- **Exceptions or risk acceptance (if applicable):**
  Approved exception details, risk owner, and expiration date

- **Current status:**
  Open, in progress, mitigated, or closed

---

11. Enforcement of Policy

Failure to comply with this policy may result in corrective actions, including but not limited to:

- Access restrictions
- Immediate review of operational procedures
- Escalation to senior management for further disciplinary action, up to and including termination

---

12. Sign-off

Chief Executive Officer (CEO):
_____ Date: _____

Chief Information Security Officer (CISO):
_____ Date: _____

Chief Information Officer (CIO):
_____ Date: _____