Vulnerability Management Process Policy

1. Purpose

The purpose of this policy is to establish and maintain a structured approach to managing vulnerabilities within the enterprise assets, ensuring that potential security weaknesses are identified, assessed, and mitigated in a timely manner.

2. Scope

This policy applies to all enterprise assets, including but not limited to hardware, software, network resources, and data. It encompasses all departments, employees, and contractors who interact with or manage these assets.

3. Policy Statement

The organization commits to a proactive and systematic approach to vulnerability management, aiming to protect enterprise assets from potential threats and minimize security risks.

4. Responsibilities

- **IT Security Team**: Responsible for overseeing the vulnerability management process, including identification, assessment, and remediation of vulnerabilities.
- **Asset Owners**: Accountable for ensuring that vulnerabilities within their assets are mitigated in accordance with the established process.
- **Employees and Contractors**: Required to comply with vulnerability management procedures and report any suspected vulnerabilities to the IT Security Team.

5. Procedures

5.1 Identification

- Perform regular scans and assessments to identify vulnerabilities in enterprise assets using approved tools and methodologies.

- Monitor security sources and feeds to stay informed of new vulnerabilities and threats.

5.2 Assessment

- Evaluate the identified vulnerabilities for their potential impact and exploitability within the enterprise environment.
- Prioritize vulnerabilities based on risk level, considering factors such as severity, asset criticality, and exposure.

5.3 Remediation

- Develop and implement remediation plans for prioritized vulnerabilities, specifying actions, timelines, and responsible parties.
- Remediation actions may include patch application, configuration changes, or compensatory controls.

5.4 Documentation

- Maintain comprehensive records of the vulnerability management process, including identified vulnerabilities, assessments, remediation actions, and outcomes.

5.5 Review and Monitoring

- Conduct periodic reviews of the vulnerability management process to evaluate its effectiveness and efficiency.
- Monitor the progress of remediation efforts and ensure timely completion.

5.6 Reporting

- Regularly report the status of vulnerability management activities to relevant stakeholders, including management and oversight bodies.

6. Compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract termination. Compliance will be monitored by the IT Security Team and reported to executive management.

7. Review and Revision

- This policy shall be reviewed and updated annually or when significant changes occur in the enterprise that could impact the vulnerability management process.
- Any amendments to the policy must be approved by the relevant authorities before implementation.

By adhering to this policy, the organization ensures a robust and effective approach to managing vulnerabilities, thus safeguarding its assets and data against potential security threats.