Vulnerability Management Policy

Version: 1.0
Last Updated: October 2025
Approved By: Chief Technology Officer (CTO)

1. Purpose

The purpose of this policy is to establish a standardized process for identifying, evaluating, prioritizing, and remediating vulnerabilities within Orbitel's infrastructure, applications, and third-party dependencies.
The goal is proactive risk reduction before threats can be exploited.

2. Scope

Applies to:

- All production, staging, and corporate systems owned or operated by Orbitel.ai.
- Cloud services, APIs, AI models, and codebases developed or deployed by Orbitel.
- Third-party software and libraries used in Orbitel's technology stack.

3. Governance and Responsibilities

- **CTO and CISO:** Jointly oversee vulnerability management strategy and remediation priorities.
- **Security Team:** Conducts vulnerability scans and penetration tests.
- **Engineering Teams:** Remediate identified issues within agreed timelines.
- **Third-Party Vendors:** Must follow Orbitel's vulnerability disclosure and patch timelines.

4. Policy Statements and Controls

a. Identification and Assessment

- Automated scanning tools perform network and application-level scans weekly.
- Static and dynamic application security testing (SAST/DAST) is integrated into the CI/CD pipeline.
- Threat intelligence feeds are monitored for newly discovered exploits or zero-days.

b. Classification and Prioritization
Vulnerabilities are ranked by **CVSS v3** score and business impact:

- *Critical (CVSS 9.0+):* Fix within 24 hours.
- *High (7.0–8.9):* Fix within 3 business days.
- *Medium (4.0–6.9):* Fix within 7 business days.
- *Low (< 4.0):* Fix within 30 days or as scheduled in the release cycle.

c. Remediation and Validation

- All patches undergo testing prior to deployment to prevent regression.
- Remediation actions are documented in Orbitel's ticketing system and tracked to closure.
- Post-fix validation ensures vulnerabilities are fully resolved.

d. Exception Management
When immediate remediation isn't feasible, temporary compensating controls (e.g., firewall rules, service restrictions) are applied and approved by the CISO.

e. External Disclosure and Bug Bounty
Orbitel maintains a **Responsible Disclosure Program**. Security researchers may report vulnerabilities to security@orbitel.ai; validated reports are acknowledged publicly after remediation.

5. Compliance and Continuous Improvement

Orbitel's vulnerability management process aligns with ISO 27001 A.8.8 and OWASP Top 10 guidelines.
Metrics on patch timeliness and recurring issues are reviewed quarterly to guide improvements.