Vulnerability and Patch Management Policy

Document ID: IE-VPP-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: IT & Engineering - Security

1. Goal

To systematically identify, assess, and remediate security vulnerabilities in all production systems, application code, and third-party dependencies.

2. Vulnerability Scanning and Assessment

- **Automated Scanning:** Continuous, automated scanning of cloud infrastructure (Cloud Security Posture Management - CSPM), container images, and application code (SAST/DAST) is mandatory.
- **Penetration Testing (Pen Test):** An external, independent penetration test must be performed **annually** against the production environment.
- **Bug Bounty Program:** A formalized bug bounty program will be maintained to engage external security researchers.

3. Remediation Timeline (Service-Level Agreement)

Vulnerabilities must be remediated according to their severity, prioritized using the Common Vulnerability Scoring System (CVSS):

CVSS Score / Severity	**Remediation Deadline**
9.0 - 10.0 (Critical)	**7 days** from discovery.
7.0 - 8.9 (High)	**30 days** from discovery.
4.0 - 6.9 (Medium)	**90 days** from discovery.
0.1 - 3.9 (Low)	Scheduled for the next quarter's technical debt sprint.

4. Patch Management

- **Operating Systems & Infrastructure:** Automated patching is enabled for non-critical infrastructure components. Manual patching for core OS kernels must occur within 14 days of a stable security release.

- **Dependencies (Code):** Library dependencies with Critical or High-severity CVEs must trigger an immediate CI/CD pipeline fix and fast-track deployment.