NepaliPay Vulnerability Management Policy

Version: 1.0
Effective Date: February 2026
Owner: Founder & Chief Executive Officer
Review Frequency: Annual

1. Purpose

This policy defines how NepaliPay identifies, prioritizes, and remediates vulnerabilities.

2. Scope

Applies to:

- Application code and dependencies
- Cloud configurations and managed services
- CI/CD pipelines and build systems

3. Approach

NepaliPay uses a risk-based approach, which may include:

- Monitoring security advisories for dependencies and vendors
- Applying security patches and dependency updates
- Reviewing changes via peer review prior to production release
- Logging and monitoring for indicators of compromise where feasible

4. Remediation and Tracking

- Triage findings and assign severity.

- Track remediation work items to closure.

- For critical issues, apply mitigations immediately where feasible and follow with permanent fixes.

5. Responsible Disclosure

Security reports can be sent to `security@nepalipay.com` .

6. Review

This policy is reviewed annually.