NepaliPay Information Security Policy

Organization: NepaliPay
Owner: Founder & Chief Executive Officer
Security Contact: security@nepalipay.com
Version: 1.0
Effective Date: February 2026
Review Frequency: Annual (or upon material changes)

1. Purpose

This policy defines the baseline security requirements NepaliPay uses to protect consumer data, financial information, and third-party integrated data (including integrations with providers such as Plaid, Stripe, and Circle).

The objective is to maintain the confidentiality, integrity, and availability of information assets.

2. Scope

This policy applies to:

- All employees, founders, and contractors
- All production and non-production environments
- Cloud-hosted infrastructure and managed services
- Source code repositories and CI/CD systems
- Consumer financial data and related metadata

3. Governance and Risk Management

NepaliPay maintains an operational information security program intended to:

- Identify and assess security risks
- Implement and validate controls
- Monitor security-relevant activity
- Respond to incidents and learn from them
- Continuously improve security posture

Program ownership:

Bidur Khatri
Founder & CEO
security@nepalipay.com

Risk assessments are conducted periodically and after major system changes.

4. Identity and Access Management (IAM)

NepaliPay enforces:

- Role-based access control (RBAC) where supported
- Least privilege access principles
- Separation between development and production access
- Centralized access management for administrative consoles
- Logging and monitoring of administrative actions where supported

Production access is restricted to authorized personnel only.

5. Multi-Factor Authentication (MFA)

Phishing-resistant MFA is required for administrative access to:

- Cloud infrastructure consoles
- Production databases and data stores

- Source code repositories
- Administrative dashboards and monitoring systems

Supported MFA methods may include authenticator apps, passkeys, and hardware devices where supported.

6. Encryption and Key Management

NepaliPay requirements:

- Data in transit uses TLS 1.2+ (or higher where supported).
- Sensitive data is encrypted at rest where supported by the platform/provider.
- Secrets (API keys, tokens, signing keys) are stored using least-privileged secret storage and are not hard-coded in source code.
- Key/secret rotation is performed after suspected exposure and periodically where feasible.

7. Infrastructure and Network Security

NepaliPay operates on managed cloud infrastructure providers and prioritizes:

- Network isolation and environment segmentation
- Managed patching and hardened configurations where supported
- Secure configuration of databases and storage
- Monitoring, logging, and alerting for security-relevant events

NepaliPay does not operate on-premises production infrastructure.

8. Secure Development Lifecycle (SDLC)

Security practices for software development include:

- Peer review for production changes

- Source control protections (e.g., protected branches) where feasible
- Dependency management and security advisories monitoring
- Secure handling of credentials and secrets in CI/CD
- Change management practices for production deployments

9. Vulnerability Management

NepaliPay follows a risk-based vulnerability management approach:

- Track and apply dependency updates
- Monitor vendor and open-source security advisories
- Prioritize remediation based on severity and exposure
- Restrict production access and continuously monitor key systems

10. Incident Response

NepaliPay maintains an incident response process to:

- Triage and contain incidents
- Investigate root cause
- Remediate and recover
- Notify affected parties where required by applicable law and agreements

See: `docs/incident-response-plan.md`.

11. Third-Party and Vendor Security

NepaliPay uses third-party service providers for certain features. NepaliPay:

- Performs due diligence appropriate to risk and data sensitivity
- Reviews security documentation and contractual terms where feasible
- Limits vendor access to least privilege

- ## 12. Policy Review

This policy is reviewed at least annually or after significant architectural changes.