NepaliPay Access Control Policy

Version: 1.0
Effective Date: [18-02-2026]
Owner: Founder & Chief Executive Officer
Review Frequency: Annual

1. Purpose

This policy defines how NepaliPay manages access to systems and data to reduce the risk of unauthorized access.

2. Scope

Applies to:

- Source code repositories and CI/CD
- Cloud consoles and managed services
- Production and non-production environments
- Administrative dashboards and monitoring systems

3. Principles

- **Least privilege:** Grant the minimum access required.
- **Need-to-know:** Limit access to sensitive data to what is necessary.
- **Separation of environments:** Restrict production access separately from development.
- **Accountability:** Use unique accounts and maintain audit trails where feasible.

4. Administrative Access

- Administrative access requires MFA where supported.
- Privileged access is limited to authorized personnel.
- Access is reviewed periodically and promptly revoked upon role change or offboarding.

5. Service Accounts and Secrets

- Use service accounts only where necessary.
- Store secrets in approved secret storage; avoid hard-coding secrets in source code.
- Rotate credentials after suspected exposure and periodically where feasible.

6. Review

This policy is reviewed annually.