NepaliPay Incident Response Plan

Owner: Founder & Chief Executive Officer
Security Contact: security@nepalipay.com
Version: 1.0
Effective Date: February 2026
Review Frequency: Annual (and after major incidents)

1. Purpose

This plan defines how NepaliPay detects, responds to, and recovers from security incidents to minimize impact to consumers, partners, and operations.

2. Scope

This plan applies to:

- The NepaliPay mobile application and supporting services
- Cloud infrastructure and production/development environments
- Third-party integrations (e.g., Plaid, Stripe, Circle) where applicable
- Employees, contractors, and service accounts with system access

3. Roles and Responsibilities

- **Incident Commander (IC):** Coordinates response, prioritization, and decisions.
- **Security Lead:** Leads technical investigation, containment, and remediation.
- **Engineering Lead:** Executes fixes, patches, rollbacks, and operational changes.
- **Comms/Support Lead:** Handles customer communications and support workflows as directed by IC.

- **Legal/Compliance (as applicable):** Advises on notification obligations and partner coordination.

For a small team, one person may fulfill multiple roles.

4. Severity Levels

- **SEV-1 (Critical):** Confirmed compromise of sensitive data, active fraud, widespread outage, or material risk to consumers.
- **SEV-2 (High):** Credible threat or partial compromise with limited scope; significant service degradation.
- **SEV-3 (Medium):** Suspicious activity or vulnerability with no confirmed impact; limited operational risk.
- **SEV-4 (Low):** Minor events, false positives, or non-exploitable issues.

5. Detection and Reporting

Incidents may be detected via:

- Monitoring and alerting (application logs, audit logs, infrastructure metrics)
- Third-party notifications (e.g., cloud provider, Plaid/Stripe/Circle)
- Customer support reports
- Internal reporting from engineers or contractors

Reporting channels:

- Email: security@nepalipay.com
- Internal escalation: notify the Incident Commander immediately for SEV-1/SEV-2

6. Response Lifecycle

6.1 Triage

- Validate the alert/report and gather initial facts
- Assign severity and roles
- Start an incident timeline and preserve key evidence

6.2 Containment

Examples (as appropriate):

- Disable or rotate affected credentials/keys
- Block suspicious traffic patterns
- Temporarily disable high-risk features
- Isolate affected services/environments

6.3 Eradication

- Identify root cause (vulnerability, leaked secret, misconfiguration)
- Remove malicious artifacts where applicable
- Patch vulnerabilities and harden configurations

6.4 Recovery

- Restore normal operations
- Validate systems (monitoring, integrity checks, smoke tests)
- Increase monitoring for recurrence

6.5 Post-Incident Review

- Document root cause and corrective actions
- Identify process/control improvements
- Track remediation items to completion

7. Evidence Handling and Logging

- Preserve relevant logs and audit trails where feasible
- Restrict access to incident artifacts to least-privileged responders
- Record all material actions taken during the incident

8. Notifications and Communications

NepaliPay evaluates notification obligations based on:

- The type of data involved
- The scope and severity of the incident
- Applicable laws and contractual requirements
- Third-party partner requirements

Communications principles:

- Provide timely, accurate, minimally speculative updates
- Coordinate external notifications through the Incident Commander
- Maintain a clear record of communications

9. Testing and Maintenance

- Perform periodic tabletop exercises (at least annually)
- Review and update this plan after significant architectural changes or incidents