Incident Response Policy

eSewa – Lyceum Group

Last Updated: June 2025

Prepared by: eSewa Infosec Team

Aligned with NIST 2.0, ISO 27001:2022, CIS 8.1, ITIL v4, 4P, and 3C Frameworks

1 Overview

Security incidents, including data breaches, malware, phishing, denial-of-service attacks, and insider threats, pose significant risks to eSewa's systems, data, and services. This policy establishes a structured framework for identifying, reporting, managing, and recovering from security incidents to ensure minimal impact, regulatory compliance, and service availability. It aligns with NIST 2.0, ISO/IEC 27001:2022, CIS Controls v8.1, ITIL v4, and the 4P (People, Process, Policy, Product) and 3C (Containment, Communication, Continuity) frameworks.

2 Purpose

The purpose of this policy is to define specific rules and requirements for managing security incidents at eSewa, a fintech company under the Lyceum Group. It ensures rapid detection, containment, eradication, recovery, and post-incident analysis while maintaining confidentiality by limiting disclosures to trusted partners and vendors to protect operational continuity.

3 Scope

This policy applies to all eSewa employees, contractors, vendors, and third-party agents accessing eSewa's information systems, networks, applications, or data. It covers all incidents affecting the confidentiality, integrity, or availability of eSewa's systems, including servers, payment APIs, and cloud environments.

4 Policy

It is the responsibility of all eSewa employees, contractors, vendors, and agents to comply with this policy during security incidents. The following actions must be taken:

1. Establish an Incident Response Team (IRT) led by the Information Security Officer, including representatives from IT/Security Operations, Legal, Compliance, Business Units, HR, and Communications as needed.
2. Conduct annual security awareness and incident response training for all employees and contractors to recognize and report incidents within 1 hour to security@esewa.com.np.
3. Maintain an updated inventory of critical assets (e.g., servers, payment APIs, AWS cloud services).
4. Implement multi-factor authentication (MFA) and role-based access controls for all systems.
5. Use encryption for data in transit and at rest, consistent with the Remote Access Policy.

6. Utilize firewalls, intrusion detection systems, anti-malware, and SIEM tools for continuous protection.
7. Maintain continuous monitoring and audit logs per CIS 8.1 standards.
8. Classify incidents by severity:
    - **Low:** Minor disruptions (e.g., phishing attempts).
    - **Medium:** Limited exposure (e.g., single-device malware).
    - **High:** Significant breach (e.g., customer PII exposure).
    - **Critical:** Widespread outage or ransomware (e.g., attack on payment APIs).
9. Share incident details only with trusted partners and vendors via encrypted channels, avoiding public disclosure unless approved by the Legal and Communications teams.
10. Prohibit:
    - Disclosing incident details to unauthorized parties without Legal team approval.
    - Tampering with logs or evidence.
    - Using eSewa resources for personal tasks during an incident.

4.1 Response Timelines

The following timelines must be adhered to for incident response actions:

Action	Timeline
Report incident to IRT	Within 1 hour
Isolate affected systems	Within 2 hours
Eradicate threat / Patch vulnerabilities	Within 24 hours (high/critical)
Restore systems from secure backups	Within 48 hours (critical)
Root cause analysis (RCA)	Within 7 days
Notify regulators (as applicable)	Within 72 hours

5 Policy Compliance

1. **Compliance Measurement**
   The Infosec Team will verify compliance through periodic audits, log reviews per CIS 8.1, employee and vendor feedback, and post-incident documentation reviews.
2. **Exceptions**
   Any exception to this policy must be approved in advance by the Information Security Officer and the Infosec Team.

3. **Non-Compliance**
   Violations may result in disciplinary action, up to and including termination of employment, and potential legal consequences for damages incurred due to data loss, service disruption, or contractual breaches.

6 Related Standards, Policies and Processes

- Acceptable Encryption Policy
- Acceptable Use Policy
- Password Policy
- Third Party Agreement
- Hardware and Software Configuration Standards for Remote Access to eSewa Networks
- Remote Access Policy

7 Acknowledgment Form

All employees and contractors must sign the following form before participating in incident response activities:

Incident Response Policy Acknowledgment

I acknowledge that I have read, understood, and agree to comply with the Incident Response Policy of eSewa.

Name: _____

Signature: _____

Date: _____

Manager/Supervisor: _____

Signature: _____

Date: _____

8 Revision History

Date of Change	Responsible	Summary of Change
June 2025	Sulav and Nikesh	Policy reviewed and approved by our chief consultant Sulav and CTO Nikesh, updated to align with NIST 2.0, ISO 27001:2022, CIS 8.1, ITIL v4, 4P, and 3C frameworks, incorporating specific actions, compliance structure, and response timelines from.