Information Security Policy Statement

Yantra Solution Private Limited, Lalitpur, Nepal

Policy Statement

Yantra Solution Private Limited is dedicated to protecting its information and information systems through robust security measures, compliance with Nepal's legal and regulatory framework, including the IT and Cybersecurity Act, 2025, and fostering a culture of security awareness. This policy provides clear guidelines to mitigate risks, maintain stakeholder trust, and ensure operational resilience in Nepal's digital landscape.

1. Protection of Confidentiality, Integrity, and Availability (CIA Triad)

Access to sensitive information is restricted to authorized personnel through strong authentication and authorization controls, compliant with the Cybersecurity Act, 2025 and industry standards. Systems and processes are designed for high availability, with measures to ensure rapid recovery from disruptions, including natural disasters common in Nepal, such as earthquakes and floods.

2. Compliance with Legal, Regulatory, and Contractual Obligations

The organization will adhere to Nepal's IT and Cybersecurity Act, 2082 (2025), Electronic Transactions Act, 2063 (2008), Individual Privacy Act, 2075 (2018), Data Act, 2079 (2022), and relevant industry standards and contractual obligations.

Non-compliance will be investigated through Root Cause Analysis (RCA), with corrective actions and periodic reviews to ensure adherence to national regulations, including mandatory breach notifications.

3. Risk and Incident Management

A risk management framework will identify, assess, and mitigate information security threats, addressing Nepal's evolving cyberthreats, such as phishing, ransomware, and data breaches, as emphasized in the IT and Cybersecurity Act, 2082 (2025).

Incident response procedures will be defined, tested, and updated to minimize incident impact, with reporting mechanisms compliant with national regulations.

Third-party risks will be managed through due diligence, effective change management procedures, contractual agreements, and regular assessments.

4. Business Continuity and Resilience

Business continuity and disaster recovery plans will be developed, maintained, and tested to ensure operational continuity during disruptions, including natural disasters and infrastructure challenges like power outages or unreliable internet.

5. Security Awareness and Training

Regular training will educate employees on security policies, Nepal-specific cyberthreats, such as social engineering targeting local businesses, and compliance with national data protection laws. - A culture of security awareness will be promoted using local languages, such as Nepali, and culturally relevant examples.

6. Data Privacy

Personal and sensitive data will be collected, processed, and stored in compliance with the Individual Privacy Act, 2075 (2018), Data Act, 2079 (2022), and IT and Cybersecurity Act 2082 (2025), ensuring informed consent and robust protection measures.

Data handling will align with Nepal's data protection framework and client requirements.

7. Building Stakeholder Trust

Transparent communication with clients, regulators, and local communities will demonstrate commitment to information security and compliance.

Engagement will reflect Nepal's cultural values of trust and collaboration.

8. Continuous Improvement

The Information Security Management System (ISMS) will be evaluated through audits, reviews, and stakeholder feedback, incorporating lessons from Nepal's cybersecurity incidents and global best practices. - Updates will reflect changes in Nepal's legal framework, including the IT and Cybersecurity Act, 2082 (2025), and emerging cyberthreats.