MONEDO FINANCIAL SERVICES PVT. LTD.

INFORMATION SECURITY MEASURES POLICY

Contents

1. Overview

This "Information Security Measures Policy" defines the specific technical and procedural controls required to protect the information assets of Monedo. This policy is drafted in accordance with applicable regulatory requirements and aligns aligned with industry-standard frameworks.

2. Objectives

- **Confidentiality:** To ensure that customer PII and financial data are accessible only to authorized personnel.
- **Integrity:** To prevent unauthorized modification of data or software.
- **Availability:** To ensure systems are resilient against cyber-attacks (e.g., Ransomware, DDoS).
- **Compliance:** To strictly adhere to RBI and CERT-In mandates regarding cyber hygiene.

3. Scope

This policy applies to:

- **Infrastructure:** All On-Premises Servers, Endpoints, Network Devices, and **Cloud Environments (SaaS, IaaS, PaaS)**.
- **Users:** All Employees, Board Members, Contractors, and Consultants.
- **Third Parties:** Must adhere to applicable security requirements.

4. Ownership

The **Chief Information Security Officer (CISO)** is the primary custodian of this policy and is responsible for defining, implementing, and maintaining security controls. Appropriate governance bodies provide oversight.

5. Responsibility for Implementation

- **IT Operations Head:** Responsible for deployment and maintenance of technical controls
- **System Administrators:** Responsible for day-to-day adherence to server security standards.

6. Reviews & Governance of Deviations

This Policy shall be reviewed periodically to ensure alignment with the changing threat landscape and applicable regulatory requirements. Any exceptions to this policy are subject to formal approval and governance

7. Communication

The HR Department and CISO shall ensure this policy is communicated to all users upon induction. All users must digitally acknowledge reading and understanding these measures annually.
Regular training and awareness programs shall be conducted for employees covering:

- Cyber hygiene practices
- Secure handling of systems
- Incident reporting procedures

8. Operational Documentation

A. Organizational Measures

To ensure that we can respond quickly to every security risk, The organization maintains structured processes to prevent and respond to cyber threats. The same has been documented briefly in the cyber security management framework. Further implementation of Information Security Management Systems (ISMS) which supports the implementation of the objectives as identified for cyber security resilience are done by the IT Team. Incidents are reported through appropriate governance channels.

B. Multiple Lines of Defense

1) Policies
2) Standard Operation Procedures
3) Metrics of Implemented procedures
4) Education and Training
5) Periodic Risk Assessment (Internal & External)

C. Risk Governance: Three Lines of Defense.

First Line (Operational Management): IT Operations staff who implement controls.
Second Line (Risk & Compliance): Designated risk and compliance functions
Third Line (Internal Audit): Independent auditors who verify the effectiveness of controls and report to appropriate governance bodies.

D. User Acceptable Use & Cyber Hygiene

- **Internet Usage:** Access to unauthorized or non-business-related websites is restricted using appropriate controls.
- In case of any suspicious emails or fraudulent activity, users must report immediately to incident@monedo.in **Phishing Awareness:** Users must not click on links from unknown sources. All suspected phishing emails must be reported immediately to incident@monedo.in.

E. Technical Security Measures

Monedo implements industry-standard technical security controls to protect systems and data.

F. Measures while browsing

To mitigate web-based threats, the following controls shall be enforced:

- Users must follow secure browsing practices and avoid unauthorized activities
- Access to malicious, high-risk, or non-business-related websites shall be restricted.
- Users shall not download unauthorized software, bypass security warnings, or disable browser security controls.
- Only organization-approved and regularly updated browsers shall be used.

Any attempt to bypass web security controls may result in disciplinary action.

G. Cross Policy Mapping

This policy shall be read in conjunction with relevant internal policies.

H. Log Management & Retention

- Logs are maintained and protected as per regulatory requirements
- Logs shall be protected against unauthorized access, modification, or deletion.

I. Regulatory Reporting

Incidents are reported to regulators in accordance with applicable requirements.

J. Risk Governance & Reporting

- Risks are tracked and reported through appropriate governance mechanisms.
- Mechanisms are in place to identify and manage :
    - Emerging risks
    - Vulnerabilities
    - Threat intelligence inputs

- Risks outside the scope of this policy must be:
    - Identified
    - Documented
    - Escalated to appropriate governance forums

K. Emerging Risk Register

Monedo shall maintain a structured repository/database of:

- Emerging cyber risks
- Risk severity classification
- Mitigation actions

L. Compliance & Enforcement

Any violation of this policy shall be addressed in accordance with **Monedo's HR Disciplinary Policy and Code of Conduct**.

Appropriate disciplinary action may be taken in accordance with applicable laws