INFORMATION TECHNOLOGY POLICY

Prepared by Legal & Compliance Team
SAMPATI SECURITIES LIMITED
2nd Floor, Mrudal Tower, B/h Times of India, Ashram Road, Ahmedabad, Gujarat, India, 380 009

Sampati Securities Limited

Information Technology Policy

1. Introduction

This Policy shall be termed as the IT Framework and Security Policy of Sampati Securities Limited ("the Company"). The terms in this Policy are defined by the Reserve Bank of India in its Master Direction on Information Technology Framework for NBFCs.

The Guidelines aim to enhance safety, security, and efficiency in IT processes, benefiting NBFCs and their customers. The Company shall conduct periodic gap analyses between its current practices and RBI stipulations, with time-bound action plans to address gaps.

2. Security Standards

The Company adopts the following security principles:

- **Confidentiality:** Access to sensitive data only by authorized users.
- **Integrity:** Accuracy and reliability of information, preventing unauthorized modification.
- **Availability:** Ensuring uninterrupted access to data and systems.
- **Authenticity:** Ensuring transactions, communications, and documents are genuine.

3. Security Aspects

- **Password Policy:** Strong passwords (minimum 6 characters, mix of upper/lowercase, numbers). No sharing or storage in plain text.
- **Access Controls:** Role-based access, least privilege principle, unique IDs for all users, auto-lock after 10 minutes of inactivity.
- **User Responsibility:** Users are accountable for all activities under their credentials.

4. Information Security

- **Asset Identification:** Maintain inventory of all IT assets with classification.
- **Role Segregation:** Role based access control – Access to information is based on well-defined user roles (system administrator, user manager, application owner.). NBFC has a clear delegation of authority to upgrade / change user profiles and permissions and also key business parameters.
- **Personnel Security:** Background checks for privileged users.

- **Physical Security:** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. NBFC has created a secured environment for physical security of information assets such as secure location of critical data, restricted access to sensitive areas li
- **Maker-Checker Principle:** Maker checker is one of the important principles of authorization in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information. NBFC ensures that it complies with this requirement to carry out all its business operations.
- **Audit Trails:** Logs for IT activities.
- **Digital Signatures:** A Digital signature certificate authenticates entity's identity electronically. NBFC protects the authenticity and integrity of important electronic documents and also for high value fund transfer.
- **Regulatory Returns** – NBFC has adequate system and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorised representatives of NBFC.
- **Cyber Threats:** Preventive and corrective measures against malware, phishing, ransomware, DDoS, and identity fraud.

5. **Cyber Security**

- NBFC takes effective measures to prevent cyber-attacks and to promptly detect any cyber intrusions to respond / recover / contain the fall out. Among other things, NBFC takes necessary preventive and corrective measures in addressing various types of cyberthreats which includes denial of service, distributed denial of services (DDoS), ransom- ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds and password related frauds.

- NBFC realises that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. NBFC ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats. Further, it also proactively promotes, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber

resilience objectives, and ensures appropriate action to support their synchronised implementation and testing

6. Confidentiality

- NBFC, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.
- Access to customer information by employees of the service provider to NBFC is on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.
- NBFC further ensures that the service provider isolates and clearly identifies NBFC's customer information, documents, records and assets to protect the confidentiality of the information. NBFC has strong safeguards in place so that there is no comingling of information / documents, records and assets.
- NBFC ensures that it immediately notifies RBI in the event of any breach of security and leakage of confidential customer related information.

7. Business Continuity Planning (BCP)

- BCP forms a significant part of any organisation's overall Business Continuity Management plan, and includes policies, standards and procedures to ensure continuity of critical business processes. BCP at NBFC is also designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.
- NBFC requires its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. NBFC ensures that the service provider periodically tests the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises with its service provider
- In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, NBFC retains an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without any break in the operations of NBFC and its services to the customers.
- NBFC ensures that service providers are able to isolate NBFC's information, documents and records and other assets. In appropriate situations, NBFC can remove, all its assets, documents, records of transactions and information given to the service provider, from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.

- These plans are also tested by NBFC on a regular basis. The results along with the gap analysis are placed with the Board.

8. Data Backup

- Daily backups of critical applications; periodically backups of file servers.
- Encrypted storage of backup copies in secure, access-controlled locations.
- Detailed records of backup movements and authorizations.
- Periodic restoration testing to validate reliability.

9. Regulatory Returns

Adequate IT infrastructure shall be maintained to file regulatory returns to RBI (Xbrl/ CIMS portal).

10. Confidentiality

- All employees shall follow confidentiality of data.
- Contractors and third-party vendors shall be bound by confidentiality clauses in formal contracts.

11. User Access Management

- Formal registration and de-registration process for system access.
- Unique IDs for users.
- Access rights revoked immediately upon termination or role change.

12. Logging & Monitoring

- Continuous monitoring of system activity.
- Logs maintained for access, changes, and incidents.

13. IT Security Reviews & Audits

- Independent audits conducted periodically.
- Risk assessments reviewed regularly.
- Findings reported to the Board with corrective actions.

14. Training & Awareness

- training programs on IT security, cyber threats, and compliance.
- Employees briefed on responsibilities before being granted access.

15. Disciplinary Process

- Formal disciplinary process for security breaches.
- Proportional response based on severity, impact, and recurrence.
- Immediate revocation of access rights in serious cases.

16. Review & Updates

This Policy shall be reviewed annually by the Board or earlier if required by regulatory changes. Updates shall be communicated to all employees and stakeholders.