Cyber Security and Cyber Resilience Policy

1. Statutory Mandate

This framework is formulated in accordance with applicable SEBI Cyber Security and Cyber Resilience guidelines including SEBI circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 dated August 20, 2024 and any amendments or substitutions issued from time to time.

The framework applies to SEBI registered intermediaries including Depository Participants, Stock Brokers and Registrar & Share Transfer Agents.

2. Objective

The objective of this framework is to ensure robust cyber security and cyber resilience in order to safeguard information systems, protect investor data and ensure uninterrupted functioning of the Company's regulated activities.

3. Applicability

This policy applies to all technology infrastructure, systems and information assets used in connection with:

- Registrar & Share Transfer Agent (RTA) operations
- Depository Participant (DP) operations
- Any other regulated activities permitted by SEBI

The policy is applicable to all employees, directors, consultants, vendors and third-party service providers who have access to the Company's information systems.

4. Scope

Cyber security refers to measures intended to protect the confidentiality, integrity and availability of computer systems, networks and data.

Cyber resilience refers to the ability of the Company to prepare for, respond to and recover from cyber incidents while continuing its business operations.

The Company shall periodically review this framework and strengthen its cyber security posture in line with technological developments and regulatory expectations.

5. Technology Environment

The Company's technology environment supporting regulated operations includes:

- Depository Participant systems hosted on infrastructure provided by NSDL.
- Registrar & Share Transfer Agent systems with data backups maintained.

- Internal operational systems maintained within the Company's office network with appropriate access controls.

6. Compliance Officer

Mr. Rajendra Kumar Mungar is designated as the Compliance Officer responsible for implementation of the cyber security framework including:

- identification and mitigation of cyber risks
- monitoring of cyber incidents
- implementation of appropriate security controls
- coordination of incident response procedures.

7. Review of Policy

The Board shall review the cyber security framework yearly and place the review on record.

The Board shall also review cyber incidents occurring globally and domestically and implement measures to strengthen cyber security controls on best effort basis.

8. Identification and Assessment of Cyber Risks

Critical IT assets shall be identified based on their importance to business operations and sensitivity of data.

These assets may include:

- servers
- data processing systems
- applications used for RTA and DP services
- network devices and IT hardware
- databases containing investor information

The IT team shall maintain an updated inventory of hardware, software, network resources and data flows.

9. Protection of Assets

Appropriate security controls shall be implemented to safeguard information assets including:

- access control mechanisms
- physical security controls
- network security management
- patch management and system hardening
- application security controls
- vulnerability assessment and penetration testing (VAPT)
- secure disposal of storage devices and systems.

10. Data Leakage Prevention

The Company shall implement appropriate safeguards to prevent unauthorized access, copying, transmission or disclosure of sensitive information handled in the course of its regulated activities.

Sensitive information may include, but is not limited to:

- investor and shareholder records
- PAN, bank account and KYC information
- corporate action data
- internal operational and financial information
- system credentials and authentication information

To mitigate the risk of data leakage, the Company shall implement the following controls:

- Access to systems and data shall be provided strictly on a **need-to-use and least privilege basis**.
- Sensitive information shall not be shared externally unless authorized and required for legitimate business or regulatory purposes.
- Storage devices such as USB drives or external media shall be used only with appropriate authorization.
- Transmission of sensitive data over public networks shall be protected through appropriate encryption or secure communication protocols.
- System logs and user activities may be monitored to detect unauthorized copying, transfer or extraction of data.
- Employees and authorized personnel shall maintain confidentiality of information and shall not disclose sensitive data to unauthorized persons.

Any suspected or actual data leakage incident shall be immediately reported to the **Compliance Officer**, who shall initiate appropriate investigation and response measures in accordance with the Cyber Security Incident Management procedures of the Company.

10. Detection and Monitoring

The Company shall implement monitoring mechanisms to detect unauthorized access, anomalies and cyber threats.

System logs, network activity and application activity shall be periodically monitored to identify suspicious behaviour or attempted intrusions.

11. Incident Response

In the event of a cyber incident:

- affected systems shall be isolated
- the incident shall be analysed and contained
- systems shall be restored from secure backups where necessary
- corrective actions shall be implemented to prevent recurrence

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall be maintained as per regulatory requirements.

12. Recovery and Continuity

Appropriate disaster recovery and backup mechanisms shall be maintained to ensure restoration of systems and continuity of operations following a cyber incident.

Periodic testing of recovery mechanisms shall be conducted.

13. Reporting Requirements

Cyber incidents and unusual activities shall be reported to the Designated Officer promptly.

Where required under regulatory guidelines, incidents shall be reported to relevant authorities including Stock Exchanges, Depositories and CERT-In.

Quarterly reports on cyber threats and incidents shall be submitted to relevant regulatory authorities as required.

14. Employee Responsibilities

Employees shall comply with cyber security procedures and assist in preventing cyber threats by:

- attending cyber security awareness programs
- protecting system credentials and passwords
- avoiding unauthorized software or devices
- reporting suspicious activities promptly.

15. Vendor Managed Systems

Where systems are managed by vendors or service providers, the Company shall ensure that such vendors comply with applicable cyber security guidelines and provide necessary certifications or assurances regarding security controls.

16. Periodic Audit

The Company shall arrange for cyber security audit of its systems annually by a CERT-In empanelled auditor or other qualified independent auditor as per SEBI circular.

Audit reports shall be reviewed by the Board.

17. Training and Awareness

Periodic training programs shall be conducted to ensure employees are aware of cyber security risks, best practices and responsibilities under this policy.