Cyber Security & Cyber Resilienc Policy

Entity Name	Manog Securities Pvt Ltd
SEBI Registration No.	INZ000278434
Designated Cyber Security Officer	Pawan Pratap Singh
Date of Adoption	28-JAN-2026

1. Policy Objective

Manog Securities Pvt Ltd adopts this Policy to protect the Confidentiality, Integrity, and Availability (CIA) of its information systems, trading infrastructure, client data, and proprietary data. Aligned with SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 and SEBI Master Circular 2025/90 paras 62–67.

2. Governance

Designated Cyber Security Officer— assesses cyber risks, implements controls coordinates incident response, and reports to the Board / Partners.

Technology Committee: constituted by Partners / Board. Reviews cyber security framework **every 6 months** and reports findings to the Board.

Annual Cyber Audit by a CERT-In empanelled auditor — report submitted to Exchange within 3 months of FY end, along with a Board/Partner declaration certifying compliance with all SEBI cyber circulars.

3. Critical Systems Inventory

System	Purpose	Internet-Facing?	Location

Registered Office : C-3/3089, Vasant Kunj, New Delhi-110070
Ph. : +91-11-42860133, 41099295, 41676280, 41824213, 41016593
E-mail : manog@manogsecurities.com

Trading Terminal	Order placement	No	On-site
RMS System	Risk monitoring	No	On-site
Back-Office Software	Reports	No	On-site

4. Five-Function Framework

4.1 Identify

- Classify all IT assets by sensitivity and criticality — maintain up-to-date inventory
- Identify cyber risks: threats, vulnerabilities, likelihood, and business impact — at least annually
- Identify third-party/vendor dependencies that may introduce cyber risk

4.2 Protect

Access Controls

- 2FA mandatory for ALL internet-facing applications — **trading portals, client login, back-office web apps, email**
- Strict need-to-use access — principle of least privilege; unique credentials per user
- User access logs: secure storage, minimum **2 years**
- Access rights reviewed quarterly — deactivated immediately on departure or role change

Network and Data Security

- Firewalls, IDS/IPS for all internet-facing infrastructure; anti-virus and anti-malware on all endpoints
- Data encrypted: in motion via TLS 1.2+; at rest via AES-256
- Critical patches applied within **72 hours**; high-severity within 14 days; medium/low within 30 days

Physical Security

- Physical access to server rooms and trading terminals restricted to authorised personnel only
- CCTV surveillance of server rooms — recordings retained for 30 days

4.3 Detect

- Continuous monitoring of security events and anomalies on all critical systems
- Installed capacity: minimum **1.5x** observed peak load of preceding calendar quarter
- Anomalies in user access patterns (unusual times, locations, failed logins) to generate automatic alerts
- Technical glitch: any unplanned outage classified and logged within **1 hour**

4.4 Respond — Mandatory Incident Reporting Timelines

Incident	Report To	Timeline	Channel
Any cyber-attack, breach, or incident	SEBI + Exchange(s)	Within 6 HOURS	sbdp-cyberincidents@sebi.gov.in + Exchange portal
Any cyber incident	CERT-In	Within 6 HOURS	CERT-In portal per CERT-In Directions 2022
Preliminary Incident Report (PIR)	Exchange(s)	T+1	Exchange incident portal
Root Cause Analysis (RCA)	Exchange(s)	Within 14 days	Exchange portal / email
Quarterly Cyber Incident Report	Exchange(s)	Within 15 days of quarter end	Annexure-25 of SEBI Master Circular 2025/90
Technical Glitch — Initial	Exchange	Within 1 hour	infotechglitch@nse.co.in
Technical Glitch — RCA	Exchange	Within 14 days	Exchange portal

4.5 Recover

- DR site: minimum **250 km** from Primary Data Centre; one-to-one hardware/software correspondence
- DR drill frequency: Annual / as per Exchange guidelines — results documented and submitted to Exchange
- All critical data backed up daily — backups stored offsite / cloud with encryption

5. Cloud Services

Cloud Services Used: **No —**

If Yes:

- All critical data stored within **India's legal boundary** — data localisation mandatory
- CSP to provide SOC-II Type II certification — reviewed annually
- SEBI Cloud Framework 9-principle GRC assessment completed before CSP engagement
- Compliance with Cloud Framework reported in cyber audit report submitted to Exchange

6. Training

- Annual cybersecurity awareness training — minimum **2 hours** for all staff
- Annual phishing simulation — minimum **once per year**
- Training records maintained for 5 years

Policy Review

Last Reviewed	**11-FEB-2026**
Reviewed By	**Pawan Pratap Singh (Compliance Officer)**
Approved By	**Director**

For and on behalf of: Manog Securities Pvt Ltd

Authorised Signatory	**Mr. Vivek Gupta**
Designation	**Director**
Date	**11-FEB-2026**
Signature	For Manog Securities Pvt. Ltd. Director