Cyber Security Policy

1. Objective

The objective of this Cyber Security Policy is to:

- Safeguard the information systems and client data of Yashwi Securities Pvt Ltd ("Yashwi" or "the Company")
- Ensure integrity, confidentiality, and availability of digital resources
- Comply with SEBI's Cybersecurity & Cyber Resilience Framework and related Exchange guidelines
- Prevent, detect, and respond to cyber threats and data breaches

2. Regulatory Framework

This policy complies with:

- **SEBI Circular SEBI/HO/MIRSD/TPD/CIR/P/2023/126** dated July 11, 2023 – *Cybersecurity and Cyber Resilience Framework for Stock Brokers and DPs*
- **Information Technology Act, 2000** (as amended)
- Exchange circulars on system security (NSE/BSE/MCX)
- CERT-In guidelines for cyber incident response

3. Scope

This policy applies to:

- All employees, vendors, associates, and third-party service providers
- All information assets and systems: servers, PCs, mobile devices, network equipment, cloud infrastructure, and software applications
- All data handled or stored including client information, transaction data, KYC documents, logs, etc.

4. Cyber Security Governance

- **Chief Information Security Officer (CISO)** is appointed to oversee cyber risk management
- **IT Security Committee** monitors cybersecurity policy compliance and reviews risks
- **Board of Directors** is kept informed of major incidents, reviews, and audit results

5. Key Components of Cybersecurity Framework

a. Access Control

- Role-based access granted on a **need-to-know basis**
- Multi-factor authentication (MFA) for all admin and sensitive user logins
- VPN access for remote employees with encryption

b. Data Protection

- Data is encrypted **in transit** (SSL/TLS) and **at rest**
- Sensitive client data masked in non-production environments
- Regular backup of data in encrypted format with **Disaster Recovery (DR)** capability

c. Endpoint Security

- Anti-virus and anti-malware software installed and updated on all endpoints
- USB and portable device usage controlled
- Devices auto-lock after defined inactivity period

d. Application & Network Security

- Web application firewalls (WAF), intrusion detection/prevention systems (IDS/IPS) in place
- Periodic **Vulnerability Assessment & Penetration Testing (VAPT)** conducted

- All software and OS patches applied promptly

e. Incident Response & Monitoring

- 24x7 real-time **security monitoring** of critical systems
- Defined **Incident Response Plan (IRP)** with roles and escalation matrix
- Cyber incidents to be reported to SEBI/Exchange/CERT-In within specified timelines

6. Cybersecurity for Client Interactions

- Secure login for clients with 2FA on trading platforms
- Client communication (emails/SMS/app notifications) digitally signed and encrypted where possible
- Clients educated on phishing, password safety, and fraud prevention

7. Third-Party Vendor Controls

- Cyber risk assessment before onboarding IT vendors
- NDA and data protection clauses in vendor agreements
- Third-party access reviewed periodically and revoked when not in use

8. User Awareness & Training

- Periodic **cybersecurity awareness training** for staff and sub-brokers
- Simulated phishing tests and cybersecurity drills
- All new hires undergo **mandatory cyber hygiene orientation**

9. Audit & Compliance

- Annual **Cybersecurity Audit** conducted by CERT-In empanelled auditors
- Logs of all security events maintained for at least **2 years**
- Findings of audits reported to Board and submitted to SEBI/exchanges

10. Business Continuity & Disaster Recovery

- DR drills conducted semi-annually
- Alternate data centre available in a different seismic zone (where applicable)
- Regular testing of backup restoration capability

11. Reporting & Disclosure

- Clients are notified in case of any data breach affecting their accounts
- Cyber incidents are reported to SEBI and exchanges per SEBI's timelines

12. Policy Review

This policy is reviewed **at least annually** or earlier in case of:

- Significant technological or regulatory changes
- Any major security incident
- Upgradation of IT infrastructure

13. Compliance Declaration

All employees, contractors, and vendors must sign a **Cybersecurity Declaration** acknowledging awareness of and compliance with this policy.