

# **Internal Control Policy**

## **1. Objective**

The purpose of this Internal Control Policy is to outline the system of controls adopted by Yashwi Securities Pvt Ltd (“Yashwi” or “the Company”) to ensure:

- Compliance with regulatory requirements
- Protection of client interests
- Prevention of fraud, misstatements, and operational risks
- Transparent and accountable business operations

This framework covers trading operations, risk management, compliance, finance, KYC, and IT systems in accordance with SEBI guidelines.

## **2. Regulatory Framework**

This policy is framed in accordance with:

- **SEBI (Stock Brokers) Regulations, 1992**
- **SEBI Master Circular for Stock Brokers (June 2023)**
- **SEBI Circulars on Risk-Based Supervision**
- **NSE/BSE/MCX Audit & Compliance Guidelines**
- ICAI’s Standard on Internal Controls (for financial reporting)

## **3. Scope of Internal Controls**

Controls have been implemented across the following functional areas:

### **a. Client Onboarding & KYC**

- Mandatory PAN, Aadhaar, and bank verification
- CKYC and e-KYC validation
- Maker-checker system for KYC approval
- Risk profiling and documentation audit before activation

**b. Order Management & Execution**

- Client orders executed only after login authentication
- Trades validated for margin, exposure, and segment eligibility
- Terminal access with user-level control and surveillance
- Automated order logs, voice logs, and audit trails maintained

**c. Risk Management Controls (RMS)**

- Margin-based exposure limits across segments
- Auto square-off mechanism for risk containment
- Real-time monitoring of MTM losses
- Separate systems for client and proprietary trades

**d. Funds and Securities Settlement**

- No co-mingling of client and proprietary funds
- Client bank accounts mapped and verified
- Daily settlement and reconciliation with exchange obligations
- Segregation of collateral (client margin pledge via NSDL only)

**e. Back Office & Accounting**

- Reconciliation of client ledger with bank and depository records
- Client statements issued weekly/monthly
- Maker-checker process for journal entries and fund payouts
- Accounting software with audit trail and password-protected access

**f. Information Security & Technology**

- Restricted access to critical IT systems and data
- Firewall, antivirus, encryption, and secure servers
- Regular system audits and data backups
- Adherence to SEBI Cybersecurity Framework (2023)

#### **g. Surveillance & Compliance**

- Real-time trade alerts for unusual volumes or price movements
- Exchange-generated alerts reviewed daily
- STR reporting under PMLA as applicable
- Internal audit, system audit, and compliance audit as per exchange schedules

#### **4. Internal Audit Mechanism**

- **Quarterly Internal Audit** by independent qualified auditors
- **System Audit** for IT infrastructure (as mandated by SEBI)
- Audit reports submitted to Board and regulators
- Follow-up on audit remarks and implementation tracked by Compliance team

#### **5. Employee Controls**

- All employees must follow a **Code of Conduct**
- Pre-clearance for personal securities trading
- Segregation of roles to avoid conflict of interest
- Training on compliance, AML, cybersecurity, and trading operations

#### **6. Whistleblower & Escalation Mechanism**

- Anonymous reporting channel for internal fraud or policy violations
- Reported to the Principal Officer or Compliance Head
- Whistleblower identity protected under confidentiality clause

## **7. Monitoring & Review**

- Daily: RMS breaches, funds mismatch, order rejections
- Weekly: Client complaints, trade errors, margin reports
- Monthly: Reconciliations, compliance checklists, internal escalations
- Annually: Policy review and update based on regulatory changes

## **8. Consequences of Control Breach**

- Internal disciplinary action
- Reporting to SEBI/Exchange where applicable
- Review of impacted process and tightening of control gaps