

## OUTSOURCING POLICY

### 1. Purpose

This Policy establishes a framework for the **identification, assessment, approval, and monitoring** of outsourcing arrangements to ensure operational efficiency, risk management, and regulatory compliance.

### 2. Scope

This Policy applies to all outsourcing arrangements of the Company, including:

- Front Office Services outsourced to Symphony Fintech Solutions Private Limited
- Back Office Services outsourced to Shilpi Computers Private Limited

### 3. Definition

Outsourcing refers to engagement of third-party service providers to perform business activities or functions that are ordinarily carried out by the Company.

### 4. Governance

- The **Board of Directors** shall approve and periodically review outsourcing arrangements.
- Senior Management shall implement this Policy and ensure compliance.

### 5. Risk Assessment & Due Diligence

Prior to entering into any outsourcing arrangement, the Company shall:

- Conduct due diligence on the service provider's financial, technical, and operational capability
- Assess risks including operational, legal, compliance, data security, and reputational risks
- Classify outsourcing as critical or non-critical

### 6. Contractual Framework

All outsourcing arrangements shall be governed by written agreements covering:

- Scope of services and service levels (SLAs)
- Confidentiality and data protection obligations
- Audit and access rights
- Business continuity and disaster recovery



- Termination and exit clauses

### 7. Monitoring and Control

- The Company shall continuously monitor performance of service providers against agreed standards
- Periodic reviews shall be conducted to assess service quality and risk exposure

### 8. Information Security

- Service providers shall maintain strict confidentiality of Company and client data
- Adequate safeguards shall be implemented to ensure data protection and cybersecurity compliance

### 9. Business Continuity

Service providers must maintain appropriate **Business Continuity Plans (BCP)** to ensure uninterrupted services.

### 10. Exit Strategy

The Company shall ensure:

- Defined exit procedures in all agreements
- Secure return or destruction of data
- Smooth transition without disruption to operations

### 11. Record Keeping

The Company shall maintain proper records of:

- Outsourcing arrangements
- Due diligence and risk assessments
- Agreements and performance reviews

### 12. Review of Policy

This Policy shall be reviewed annually or as required to ensure continued relevance and compliance.

For CapitalSquare Financial Services Pvt. Ltd.

  
Authorized Signatory

\*\*\*\*\*



## Internal Control Policy

### 1. Purpose

The purpose of this Internal Control Policy is to establish a robust framework of controls, processes, and procedures to ensure:

- Efficient and orderly conduct of business
- Safeguarding of assets and client securities
- Prevention and detection of fraud and errors
- Accuracy and reliability of financial and operational reporting
- Compliance with applicable laws and regulations

### 2. Scope

This policy applies to:

- All departments and business functions
- Employees, directors, authorised persons, and agents
- Third-party service providers and vendors engaged in operations

### 3. Control Environment

The Company shall maintain a strong control environment based on:

- Ethical governance and tone from the top
- Clearly defined organisational structure
- Segregation of duties
- Accountability at all levels
- Compliance culture embedded across operations

### 4. Key Internal Control Principles

#### 4.1 Segregation of Duties

No single individual shall control all aspects of a transaction. Key functions shall be separated as follows:

- Front Office (Client acquisition & trading)
- Middle Office (Risk & compliance monitoring)
- Back Office (Settlement, reconciliation, accounting)



#### **4.2 Authorization & Approval Controls**

- All transactions must be properly authorised
- Defined approval matrix for financial and operational decisions
- High-value or sensitive transactions require senior management approval

#### **4.3 Record Keeping & Documentation**

- All transactions must be accurately recorded
- Supporting documents must be maintained in physical or electronic form
- Records must be retained as per regulatory requirements

#### **4.4 Access Controls**

- Role-based system access shall be enforced
- Restricted access to sensitive data and trading systems
- Periodic review of user access rights
- Immediate revocation of access upon employee exit

### **5. Operational Controls**

#### **5.1 Client Onboarding Controls**

- Mandatory KYC verification before account activation
- Proper documentation and audit trail
- Approval from compliance team before activation

#### **5.2 Trading Controls**

- System-based validation of client orders
- Prevention of unauthorized trading
- Monitoring of abnormal trading patterns
- Segregation of proprietary and client trades

#### **5.3 Settlement Controls**

- Daily reconciliation of client funds and securities
- Timely settlement with exchanges and depositories
- Exception reporting for discrepancies



#### **5.4 Reconciliation Controls**

- Daily reconciliation of:
  1. Bank accounts
  2. Trading positions
  3. Client ledgers
  4. Exchange records
- Investigation of mismatches without delay

#### **6. Financial Controls**

- Proper accounting and bookkeeping systems
- Monthly financial closing and review
- Budgetary control and expense approvals
- Audit trails for all financial transactions
- Prevention of unauthorized payments

#### **7. Compliance Controls**

The Company shall ensure compliance with:

- SEBI regulations
- Rules of National Stock Exchange of India and BSE Limited
- Anti-Money Laundering (AML) requirements
- Internal policies including COI, Risk, and AP policies

Compliance Officer shall conduct regular monitoring and reporting.

#### **8. Risk Management Integration**

Internal controls shall be aligned with the Risk Management Framework to:

- Identify operational and financial risks
- Implement preventive controls
- Monitor risk indicators
- Escalate significant issues to management

#### **9. Fraud Prevention & Detection**

The Company shall implement:



- Whistleblower mechanism for reporting fraud
- Surprise audits and inspections
- Monitoring of employee and AP activities
- System alerts for suspicious transactions
- Immediate investigation of red flags

#### **10. Technology & System Controls**

- Secure IT infrastructure with firewalls and encryption
- Regular system backups and disaster recovery setup
- Change management controls for system updates
- Cybersecurity monitoring and incident response mechanisms

#### **11. Vendor & Outsourcing Controls**

- Due diligence before onboarding vendors
- Written agreements with service level commitments
- Periodic performance review
- Monitoring of outsourced activities
- Control over data access and confidentiality

#### **12. Internal Audit**

- Independent internal audit function shall be established
- Risk-based audit plan approved by management/board
- Periodic audits of all critical functions
- Reporting of findings with corrective action plans (CAPA)
- Tracking of closure of audit observations

#### **13. Reporting & Escalation**

- Daily/weekly operational MIS reporting
- Immediate escalation of material deviations
- Reporting of critical incidents to senior management
- Quarterly review of control effectiveness



#### 14. Training & Awareness

- Mandatory training on internal controls for employees
- Awareness sessions on fraud prevention and compliance
- Periodic updates on regulatory and process changes

#### 15. Review & Update of Policy

This policy shall be reviewed:

- Annually
- After regulatory changes issued by SEBI or exchanges
- Following major operational or organizational changes

For CapitalSquare Financial Services Pvt. Ltd.

  
Authorised Signatory

