

ONLINE BUSINESS AND PREVENTION POLICY (OBPP)

1. Objective

The objective of this Policy is to establish controls for online business activities, client onboarding, internet-based trading services, and prevention of unauthorized access, fraud, cyber threats, and misuse of online trading facilities. The policy aims to ensure compliance with SEBI, Stock Exchange, Depository, and other applicable regulatory requirements.

2. Scope

This Policy applies to:

- Online account opening
- Internet and mobile trading platforms
- Digital KYC and e-KYC processes
- Client authentication
- Online fund transfer facilities
- Online document execution
- User access management
- Employees and Authorised Persons involved in online business

3. Client Onboarding

The Trading Member shall:

- Verify client identity through prescribed KYC procedures.
- Complete IPV (In-Person Verification) through approved methods.
- Verify PAN, Aadhaar (where applicable), bank account, email ID and mobile number.
- Obtain client consent electronically wherever permitted.
- Ensure successful KRA and CKYCR verification before account activation.

4. Client Authentication

Clients shall access online trading only after successful authentication through:

- Unique User ID
- Strong Password
- Two-Factor Authentication (2FA)
- OTP-based verification wherever applicable

Passwords shall never be shared with any employee or third party.

5. Online Trading Controls

The Trading Member shall ensure:

- Secure login mechanism

- Encrypted communication
- Automatic session timeout
- Audit trail of all login activities
- Real-time order monitoring
- Order confirmation before execution
- System logs maintained as per regulatory requirements

6. Prevention of Unauthorized Access

The Member shall implement:

- Role-based access controls
- Periodic password changes
- Multi-factor authentication for privileged users
- Restricted administrative access
- Antivirus and Endpoint Protection
- Firewall protection
- Intrusion detection and prevention systems
- Regular vulnerability assessments

7. Cyber Security Controls

The Member shall:

- Maintain cyber security framework.
- Conduct periodic Vulnerability Assessment and Penetration Testing (VAPT).
- Monitor security logs.
- Patch critical vulnerabilities promptly.
- Maintain secure backups.
- Perform periodic restoration testing.
- Report cyber incidents as per regulatory timelines.

8. Client Communication

Clients shall receive:

- OTPs
- Trade confirmations
- Contract Notes
- Margin statements
- Ledger statements
- Holding statements
- Login alerts
- Password reset alerts

through registered email IDs or mobile numbers.

9. Prevention of Fraud

The Trading Member shall monitor for:

- Suspicious login attempts
- Multiple failed login attempts
- Unusual trading patterns
- Unauthorized fund transfers
- Fake websites and phishing
- Identity theft
- System misuse

Appropriate preventive and corrective actions shall be taken immediately.

10. User Responsibilities

Clients shall:

- Maintain confidentiality of login credentials.
- Immediately report unauthorized access.
- Regularly update passwords.
- Verify trade confirmations.
- Report discrepancies promptly.

11. Employee Responsibilities

Employees shall:

- Follow Information Security Policy.
- Maintain confidentiality.
- Report security incidents immediately.
- Avoid sharing passwords.
- Access systems strictly on a need-to-know basis.

12. Incident Management

The Trading Member shall:

- Maintain an Incident Response Plan.
- Record all incidents.
- Investigate root causes.
- Take corrective actions.
- Notify regulators wherever required.
- Preserve forensic evidence.

13. Business Continuity

The Member shall maintain:

- Disaster Recovery Site

- Data Backup Procedures
- Business Continuity Plan
- Periodic DR Drills
- Recovery Time Objectives as prescribed

14. Record Retention

The Member shall retain:

- Login logs
- System logs
- Order logs
- Client communications
- Security incident records
- Audit reports

for the period prescribed under SEBI and Exchange regulations.

15. Compliance Monitoring

The Compliance Officer and Information Security Team shall periodically review:

- User access
- Cyber security controls
- Online onboarding processes
- Regulatory compliance
- Vendor compliance
- Incident reports

16. Review of Policy

This Policy shall be reviewed at least annually or earlier if required due to:

- Changes in SEBI regulations
- Exchange circulars
- Cyber security advisories
- Changes in business operations

17. Approval

This Policy has been approved by the Board of Directors of **M/S ARJ Securities Pvt. Ltd.** and shall be effective from **11/09/2026**.