

ELECTRONIC COMMUNICATION POLICY

Effective Date: As per SEBI Circular | **Classification:** Mandatory Compliance | **Applies to:** All Trading Clients

1. PREAMBLE & PURPOSE

Bullsmart Financial Services Private Limited ('Bullsmart' or 'the Company'), operator of the mobile trading application Bullsmart, is a SEBI-registered stock broker committed to maintaining the highest standards of regulatory compliance, investor protection, and professional conduct in all its electronic communications.

This Electronic Communication Policy ('Policy') is formulated in accordance with:

- Securities and Exchange Board of India (Stock Brokers) Regulations, 1992
- SEBI Master Circular for Stock Brokers (latest version)
- The Information Technology Act, 2000 and IT (Amendment) Act, 2008
- IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- NSE, BSE, and MCX exchange circulars on electronic communications
- SEBI Circular on Code of Conduct for Stock Brokers

This Policy establishes the framework governing all electronic communications conducted by Bullsmart, its directors, officers, employees, contractors, and agents, whether through the Bullsmart mobile application, official email systems, or any other electronic medium.

2. SCOPE & APPLICABILITY

2.1 Personnel Covered

- All full-time and part-time employees of Bullsmart Financial Services Pvt. Ltd.
- Contract staff, consultants, and third-party service providers with access to company systems
- Directors and senior management
- Relationship managers, dealer terminal operators, and customer-facing staff
- IT personnel and system administrators

2.2 Communication Channels Covered

- Bullsmart Mobile Application (iOS and Android platforms)
- Official corporate email systems (@bullsmart.in domain)
- SMS and automated alert systems
- Push notifications via the Bullsmart app

- Web-based trading portals
- Instant messaging via officially sanctioned platforms only
- Electronic Contract Notes (ECNs)
- Automated order confirmation and trade confirmation messages

2.3 Communication Channels Explicitly Prohibited

Prohibited Channel	Reason for Prohibition
Personal WhatsApp / Signal / Telegram	Non-auditable; cannot be archived per SEBI norms
Personal email accounts (Gmail, Yahoo, etc.)	No corporate control; encryption non-compliant
Social media (Twitter/X, Facebook, LinkedIn DMs)	Public or semi-public; investor protection risk
Unofficial group chats or forums	Cannot ensure non-tamperable audit trail
Unrecorded voice notes / calls for trade	Violates recording obligations under SEBI norms

3. MANDATORY REGULATORY REQUIREMENTS

3.1 Recording & Archiving of Communications

In compliance with SEBI's requirements for maintaining a non-tamperable audit trail, Bullsmart shall:

- Record all trading instructions and confirmations received through the Bullsmart mobile application
- Maintain tamper-proof electronic logs of all client-facing communications for a minimum of 5 years
- Ensure all records are stored in a non-editable, time-stamped, encrypted format
- Maintain records on secure servers with automated daily backups and disaster recovery provisions
- Provide the stock exchanges and SEBI access to such records upon demand within 24 hours of requisition

3.2 Electronic Contract Notes (ECNs)

All Electronic Contract Notes issued through the Bullsmart platform must:

- Be digitally signed using a valid Digital Signature Certificate (DSC) issued by a SEBI-recognised Certifying Authority
- Be encrypted using minimum AES-256 bit encryption standards
- Be non-tamperable and carry a unique reference number
- Be delivered to the client's registered email address within 24 hours of trade execution
- Comply with the IT Act, 2000 requirements for electronic records and digital signatures

- Contain all mandatory disclosures as specified by the relevant stock exchange circular

3.3 Client Data Accuracy & Updates

- Bullsmart shall maintain accurate and current client contact information including mobile numbers and email
- addresses
- Clients shall be prompted to verify and update contact details during the annual KYC re-verification process
- Automated alerts, margin calls, and contract notes shall only be sent to SEBI KYC-verified contact details
- Any request for change in client communication details shall be processed only after two-factor authentication

3.4 Cybersecurity & Data Protection

- The Bullsmart mobile application shall comply with SEBI's Cyber Security and Cyber Resilience Framework (CSCRF)
- All communications through the Bullsmart app shall use end-to-end TLS 1.2 or higher encryption
- Multi-factor authentication (MFA) shall be mandatory for all client logins and transaction authorisations
- Regular penetration testing of the communication infrastructure shall be conducted at least once every six months
- Data classification protocols shall be implemented to safeguard Sensitive Personal Data or Information (SPDI) under IT Rules, 2011

4. PERMITTED & MANDATED CLIENT COMMUNICATIONS

The following communications shall be sent to clients through the Bullsmart mobile application and/or registered email/SMS only:

Sr. no.	Communication Type	Channel	Frequency / Trigger
1	Trade Confirmation / Order Execution Alert	App Push Notification + SMS	Immediately upon execution
2	Electronic Contract Note (ECN)	Registered Email	Within 24 hours of trade
3	Margin Call / Shortfall Notice	App Notification + SMS + Email	Real-time / as required
4	Account Statement	Registered Email + App	Monthly / on demand
5	Risk Disclosure Statement	Email + App	Account opening & annually
6	Password / OTP Alerts	Registered Mobile (SMS)	On each login / transaction
7	DEMAT Holdings Statement	Registered Email	On request / quarterly

8	Regulatory Announcements	App Notification + Email	As applicable
9	Dividend / Corporate Action Alerts	App Notification	On occurrence
10	Grievance Acknowledgement	Email + App	Within 24 hours of complaint

5. PROHIBITED CONDUCT & MISUSE PREVENTION

The following conduct is strictly prohibited and may attract disciplinary action, including termination and regulatory reporting:

- Sharing client account information, portfolio details, or personal data over personal messaging platforms
- Receiving or acting upon trading instructions from clients via personal WhatsApp, personal email, or any non-approved channel
- Sending investment advice, stock tips, research recommendations, or trading calls through personal communication devices
- Soliciting clients for transactions outside the Bullsmart platform or official communication channels
- Forwarding internal communications, client data, or trade information to personal devices or external parties without authorisation
- Using communication channels to engage in front-running, insider trading, or market manipulation
- Impersonating Bullsmart or its officials in any communication medium
- Sharing login credentials, OTPs, or access tokens with any individual, including colleagues

5.1 Disciplinary Consequences

Violation Level	Consequence
First instance — minor breach	Written warning + mandatory re-training
Second instance — moderate breach	Suspension (unpaid) + compliance review
Serious breach — data leakage / client fraud	Termination + regulatory reporting to SEBI/Exchange
Criminal conduct — market manipulation / fraud	Termination + FIR + regulatory prosecution

6. STAFF TRAINING & COMPLIANCE PROGRAMME

6.1 Mandatory Training Requirements

All personnel covered under Section 2.1 shall undergo mandatory Electronic Communication Compliance Training (ECCT) as follows:

- Induction Training: Completion required within 7 working days of joining
- Annual Refresher Training: Mandatory once every financial year for all existing staff
- Post-Amendment Training: Required within 30 days of any material amendment to this Policy or relevant SEBI circulars
- Role-Specific Training: Additional module for dealer terminal operators, relationship managers, and IT staff

6.2 Training Delivery via Bullsmart App

Training shall be primarily delivered through a dedicated Compliance Training Module within the Bullsmart internal staff portal, complemented by:

- Interactive video modules (minimum 45 minutes per session)
- Case study-based scenarios drawn from SEBI enforcement actions
- Policy quiz (see Section 7) with a minimum passing score of 75%
- Digital acknowledgement of policy receipt and understanding

6.3 Training Records & Audit

- The Compliance Officer shall maintain a Training Register with dates, scores, and acknowledgements for each employee
- Training completion records shall be produced during SEBI/Exchange inspections as evidence of compliance awareness
- Employees failing the quiz shall undergo remedial training and re-assessment within 5 working days

7. GRIEVANCE REDRESSAL & REPORTING

7.1 Reporting Violations

Any employee who becomes aware of a breach or suspected breach of this Policy must:

- Report the matter immediately to the Compliance Officer via the official internal reporting mechanism or email: compliance@bullsmart.in
- Not attempt to investigate or rectify the breach independently
- Preserve all relevant communication records and not delete, modify, or share them
- Cooperate fully with any internal investigation or regulatory inquiry.

7.2 Whistleblower Protection

Bullsmart is committed to protecting employees who report violations in good faith. No employee shall face retaliation, discrimination, or adverse employment action for reporting a

genuine concern under this Policy. Anonymous reporting may be made to the Compliance Officer or through the SEBI SCORES portal.

7.3 Client Complaints

Clients experiencing issues with electronic communications may raise grievances through:

- Bullsmart App: Help & Support section
- Email: grievance@bullsmart.in
- SEBI SCORES Portal: scores.gov.in
- Stock Exchange investor grievance portals (NSE IGRC / BSE Investor Portal)

8. POLICY REVIEW & AMENDMENT

This Policy shall be reviewed annually by the Compliance Officer and the Board of Directors. Amendments shall be necessitated by:

- Material changes in SEBI regulations, circulars, or exchange guidelines
- Significant technological changes in the Bullsmart platform
- Findings from internal or external audits
- Regulatory inspections or enforcement actions

All amendments shall be communicated to staff within 15 working days and shall trigger a mandatory refresher training session.