

CYBER SECURITY AND PHISHING AWARENESS ADVISORY POLICY

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

PART A — INTERNAL CYBER SECURITY POLICY (SEBI CSCRf Compliant)

A1. Preamble & Regulatory Framework

Skywards Investec Private Limited ('Skywards Investec'), operator of the Bullsmart mobile trading platform, is a SEBI-regulated entity (RE) and is subject to the Cybersecurity and Cyber Resilience Framework (CSCRf) issued by SEBI vide Circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/xxx dated August 20, 2024, as updated by Clarification Circulars dated April 30, 2025 and August 28, 2025.

CSCRf replaces all previous SEBI cybersecurity and cyber resilience circulars issued for stock brokers. The CSCRf is built on five Cyber Resilience Goals: ANTICIPATE, WITHSTAND, CONTAIN, RECOVER, and EVOLVE. This Policy incorporates all seven regulatory pillars mandated by SEBI CSCRf and is structured accordingly.

A1.1 RE Categorisation of Skywards Investec under CSCRf

CSCRf adopts a graded approach and categorises REs based on size, number of clients, and trading volume. The applicable category for Skywards Investec is determined as follows:

Category	Threshold Criteria	Key Additional Requirements
Market Infrastructure Institutions (MIIs)	NSE, BSE, MCX, Clearing Corps, Depositories	Mandatory C-SOC; Red Teaming; VAPT twice a year; ISO 27001 mandatory
Qualified REs	Active clients >50 lakh; or Traded Value >Rs.20,000 Cr/month (cash); or >Rs.2,50,000 Cr/month (F&O)	In-house/Group SOC or third-party SOC; VAPT twice a year; Red Teaming; ISO 27001; IT Committee with external expert
Mid-size REs	Active clients between 10 lakh and 50 lakh; or trading value thresholds between Qualified and Small	SOC (in-house/third-party/M-SOC); VAPT once a year; Cyber Audit twice; IT Committee
Small-size REs	Active clients below 10 lakh and trading value below Mid-size thresholds	Can use NSE/BSE Market SOC (M-SOC); VAPT once a year; Cyber Audit once; IT Committee
Self-Certification REs	Smallest entities — minimal cyber exposure	Self-certification; periodic vulnerability assessments; no standalone SOC mandatory

A2. Pillar 1 — Governance & Leadership

A2.1 Board Ownership & Policy Approval

- This Cyber Security Policy has been approved by the Board of Directors of Skywards Investec Private Limited, in accordance with SEBI CSCRF which mandates that the cybersecurity policy be owned and approved by the Board of Directors / Partners / Proprietor
- The Board shall review and re-approve this Policy annually and whenever material changes are made
- The Board shall be briefed on the state of cybersecurity, significant incidents, and CSCRF compliance status at every Board Meeting
- A copy of the Board-approved Policy shall be submitted to the relevant Stock Exchanges as part of CSCRF compliance reporting

A2.2 Chief Information Security Officer (CISO)/Senior Level Employee

In compliance with SEBI CSCRF:

- Skywards Investec has designated a senior official as the Chief Information Security Officer (CISO), whose grade and standing shall be at least equivalent to the CTO/CIO of the Company
- The CISO shall report directly to the MD/CEO (or to the Board of Directors as per the organisational structure of Skywards Investec)
- The CISO is accountable for the implementation, monitoring, and continuous improvement of this Cyber Security Policy
- The CISO's name, designation, and contact details shall be published on the Bullsmart website and communicated to the relevant Stock Exchange
- The CISO shall prepare a Cybersecurity Status Report for the Board at minimum on a half-yearly basis

A2.4 Policy Review Cycle

- This Policy shall be reviewed annually by the CISO and IT Committee, and approved by the Board of Directors
- Out-of-cycle reviews shall be triggered by: (a) new or amended SEBI CSCRF circulars; (b) significant cyber incidents; (c) major changes to the Bullsmart platform's technology infrastructure; (d) findings from cyber audits or VAPT
- Versions of this Policy shall be maintained with dates of approval; superseded versions shall be archived for 5 years.

A3. Pillar 2 — Identification & Classification of Assets

A3.1 Asset Inventory

- Skywards Investec shall maintain a comprehensive, up-to-date asset inventory covering: all hardware (servers, network devices, endpoints, mobile devices); all software (applications, operating systems, databases, third-party tools); all information assets (client data, trade data, market data); and all cloud-based and SaaS resources

- The asset inventory shall be reviewed and updated at least quarterly and after every major infrastructure change
- A Software Bill of Materials (SBOM) shall be maintained as mandated by SEBI CSCRF to track all software components deployed in the Bullsmart platform
- Internet-facing applications and systems, including the Bullsmart mobile app and web portal APIs, shall be identified and specifically flagged in the inventory

A3.2 Data Classification

All data handled by Skywards Investec shall be classified based on sensitivity as follows:

Classification	Examples	Controls Required
Highly Confidential	Client PAN, Aadhaar, bank account details, passwords, trading credentials, demat account data	End-to-end encryption at rest and in transit; access on strict need-to-know basis; data localisation in India mandatory; DLP controls mandatory
Confidential / Sensitive	Trade data, portfolio information, client correspondence, KYC documents, SEBI filings	Encryption; access controls; audit logging; cannot be transmitted outside India without SEBI approval
Internal	Internal policies, operational procedures, staff records, vendor contracts	Access restricted to authorised employees; password protection; no public sharing
Public	Published policies, investor charter, SEBI registration details	No special restrictions: but integrity controls required

A3.3 Identification of Critical Systems

- Skywards Investec shall maintain a list of 'Critical Systems' including: Bullsmart trading platform (order management system); client authentication systems; electronic contract note (ECN) generation system; fund transfer and settlement systems; DDPI-based demat debit systems; client data storage (KYC and trade data); IRRA connectivity; Exchange connectivity (FIX/co-location links)
- As per SEBI CSCRF Clarification (Apr 30, 2025), the definition of Critical Systems has been expanded to include systems integral to business continuity, all client-facing applications, and systems connected to core operational networks
- Critical Systems shall receive enhanced security controls, more frequent VAPT, and priority treatment in BCP/DR planning.

A4. Pillar 3 — Protection & Technical Defences

A4.1 Access Controls & Authentication

- Multi-Factor Authentication (MFA) is mandatory for all users — employees, contractors, and clients — accessing any Skywards Investec system, particularly for remote access, VPN connections, and critical systems
- Role-Based Access Control (RBAC) shall be implemented — users shall be granted the minimum access necessary for their role (Principle of Least Privilege)

- Privileged Access Management (PAM): Privileged accounts (admin/root) shall be separately managed, logged, and reviewed quarterly
- All Bullsmart client sessions enforce 2FA on every login as mandated by SEBI/Exchange IBT guidelines
- Authentication logs shall be maintained centrally and retained for minimum 5 years
- Periodic access reviews shall be conducted — quarterly for privileged accounts and semi-annually for general user accounts; access shall be revoked within 24 hours of employee separation

A4.2 Network Security

- Network segmentation shall be implemented to isolate sensitive systems (trading systems, client data stores) from general office networks and internet-facing systems
- Firewalls shall be deployed at all network perimeters with rule sets reviewed quarterly
- Web Application Firewall (WAF) shall be deployed to protect the Bullsmart web portal and all public-facing APIs from OWASP Top 10 vulnerabilities, injection attacks, DDoS, and bot traffic
- Intrusion Detection and Prevention Systems (IDS/IPS) shall be deployed to monitor and block malicious network traffic
- All wireless networks used for business purposes shall be secured with WPA3 encryption; guest and business Wi-Fi shall be on separate SSIDs with network isolation
- API security shall be implemented with OAuth 2.0-based access control, rate limiting, throttling, and proper authentication/authorisation mechanisms as mandated by SEBI CSCRF
- All VPN connections for remote access shall enforce MFA and use strong encryption

A4.3 Encryption

- All Highly Confidential and Confidential data at rest shall be encrypted using AES-256 bit encryption or equivalent standard
- All data in transit (internal and external) shall use TLS 1.2 or higher; TLS 1.0 and 1.1 shall be disabled
- Full Disk Encryption (FDE) shall be implemented on all laptops, mobile devices, and servers handling sensitive data
- File-based Encryption (FE) shall be layered with FDE for additional protection of critical files as required by SEBI CSCRF
- Encryption keys shall be managed within India (data localisation); routing encrypted data through servers outside India violates SEBI's data sovereignty expectations
- Post-quantum cryptography solutions shall be evaluated as part of the annual policy review to address future quantum computing threats

A4.4 Data Loss Prevention (DLP)

- DLP solutions shall be deployed to prevent unauthorised transmission of Highly Confidential and Confidential data outside the Skywards Investec environment
- DLP policies shall cover email, USB/removable media, cloud uploads, and screen capture
- Any DLP policy violation shall trigger an automated alert to the CISO and be logged for investigation

A4.5 Endpoint Security

- Endpoint Detection and Response (EDR) solutions shall be deployed on all endpoints (laptops, desktops, servers)
- Mobile Device Management (MDM) solution shall be used for managing corporate mobile devices used by employees
- Employees are prohibited from accessing Skywards Investec systems from personal devices that do not meet the company's security standards
- Anti-malware and anti-ransomware software shall be installed and maintained with up-to-date signatures on all endpoints

A4.6 Secure Development Lifecycle (SDLC) for Bullsmart App

- Security testing (including DAST — Dynamic Application Security Testing) shall be integrated into the Bullsmart app development lifecycle
- Security testing shall be conducted before every major release and after any major system change, as required by SEBI CSCRF guidelines PR.IP.S4 and PR.IP.S6
- Business logic vulnerabilities and hidden vulnerabilities that automated scans may miss shall be assessed through manual penetration testing
- Third-party libraries and components used in the Bullsmart app shall be tracked via SBOM (Software Bill of Materials) and assessed for known vulnerabilities

A5. Pillar 4 — Detection & Monitoring

A5.1 Security Operations Centre (SOC)

SOC Requirement	Details
SOC Mandate	All SEBI-regulated entities (except the smallest Self-Certification REs) are required to establish SOC mechanisms for continuous monitoring of security events
SOC Options	Skywards Investec may maintain: (a) In-house SOC; (b) Group entity SOC; (c) Third-party managed SOC; (d) NSE/BSE Market SOC (M-SOC) — as appropriate for Skywards Investec's category
M-SOC Availability	NSE and BSE have established Market SOCs (M-SOC) to provide cybersecurity monitoring to smaller entities that cannot maintain their own SOC
SOC Functions	24x7 monitoring of security events; threat detection; anomaly detection; alert triage; incident escalation; log analysis

SOC Efficacy	MIIs and Qualified REs: measure SOC functional efficacy half-yearly. Other REs: obtain SOC efficacy assessment annually from SOC service providers, using SEBI CSCRF's quantifiable method and indicative parameter list
Log Retention	Centralised logging of all security events; logs retained for minimum 5 years in tamper-proof format as required by SEBI CSCRF

A5.2 Centralised Log Management & Monitoring

- Centralised Security Information and Event Management (SIEM) shall be used to aggregate and correlate logs from firewalls, routers, switches, IDS/IPS, servers, and the Bullsmart application
- An authentication and access policy along with effective log collection and retention policy shall be documented and implemented as required by SEBI CSCRF
- Security devices (firewalls, routers, IDS/IPS) shall be monitored continuously for anomalous activity
- User activity monitoring shall be implemented for privileged account holders; all admin actions on critical systems shall be logged

A5.3 Phishing & Impersonation Monitoring

- Skywards Investec shall proactively scan cyberspace for phishing websites, fake mobile apps, and social media accounts impersonating the Bullsmart brand or Skywards Investec
- Upon detection of a phishing website or fake Bullsmart app, Skywards Investec shall immediately: (a) report to CERT-In at incident@cert-in.org.in; (b) initiate takedown procedures with the hosting provider and app store; (c) notify SEBI; (d) alert clients via the official Bullsmart platform
- Phishing simulation exercises shall be conducted for all employees at least twice a year to test and improve human resilience against social engineering.

A6. Pillar 5 — Response & Recovery

A6.1 Cyber Incident Response Plan (IRP)

- Skywards Investec shall maintain a comprehensive, documented Cyber Incident Response Plan (IRP) as mandated by SEBI CSCRF
- The IRP shall cover: Detection and Classification; Containment; Eradication; Recovery; Post-Incident Root Cause Analysis (RCA) and Lessons Learned
- Incident Severity Levels shall be defined (P1 Critical / P2 High / P3 Medium / P4 Low) with specific response timelines and escalation procedures for each
- The IRP shall identify the incident response team with clearly defined roles, responsibilities, and contact details
- Forensic investigation capabilities shall be available (in-house or via contracted third party) for detailed investigation of material cyber incidents
- Tabletop simulation drills and incident response exercises shall be conducted quarterly to test the IRP's effectiveness

A6.2 Incident Reporting Timelines

Incident Type	Report To	Timeline
All cyber incidents (breach, ransomware, DDoS, data leak, system compromise)	SEBI via SEBI Incident Reporting Portal + CERT-In	Within 6 hours of detection
Significant incidents impacting client data or trading operations	Stock Exchanges (NSE/BSE/MCX) + SEBI	Within 6 hours; follow-up report within 72 hours
Phishing websites / fake apps targeting Skywards Investec	CERT-In (incident@cert-in.org.in) + Stock Exchanges + SEBI	Within 24 hours of detection
Post-incident Root Cause Analysis (RCA) report	SEBI + relevant Exchange	Within 30 days of incident closure

A6.3 Cyber Crisis Management Plan (CCMP)

- Skywards Investec shall maintain an up-to-date Cyber Crisis Management Plan (CCMP) as required by SEBI CSCRf
- The CCMP shall define escalation paths, external communication protocols (SEBI, exchanges, law enforcement, media), and decision-making authority during a cyber crisis
- CCMP shall be tested through tabletop exercises at least quarterly

A6.4 Business Continuity & Disaster Recovery (BCP/DR)

- Skywards Investec shall maintain a Primary Trading System and a Disaster Recovery (DR) site for the Bullsmart platform as mandated by SEBI CSCRf
- Recovery Time Objective (RTO): Critical operations must achieve a maximum 2-hour RTO as mandated by SEBI CSCRf Clarification (April 30, 2025)
- Recovery Point Objective (RPO): Critical data must achieve a maximum 15-minute RPO
- BCP/DR plans shall be tested at least twice a year through drills; results shall be documented and remediation actions tracked
- The IRRA (Investor Risk Reduction Access) platform participation is a component of Skywards Investec's client-facing business continuity framework — ensuring clients can square off positions even during Bullsmart system outages.

A7. Pillar 6 — Third-Party & Vendor Risk Management

A7.1 Vendor / Third-Party Risk Assessment

- All third-party vendors providing technology services to Skywards Investec (cloud service providers, SaaS vendors, managed SOC providers, KRA connectivity, data feed providers) shall undergo a comprehensive security assessment before engagement and annually thereafter
- Contracts with technology vendors shall mandate compliance with SEBI CSCRf and applicable data protection regulations, and shall include provisions for security audits and incident notification

- Third-party access to Skywards Investec systems shall be granted on a need-to-know basis, time-limited, and fully logged
- Supply chain risk management is explicitly highlighted in SEBI CSCRF — Skywards Investec shall maintain awareness of the cybersecurity posture of its technology supply chain

A7.2 Cloud Service Provider (CSP) Obligations

- Use of cloud services (IaaS, PaaS, SaaS) shall comply with SEBI's Cloud Adoption Framework
- Contractual/agreement terms with CSPs shall clearly specify provisions for sharing audit reports including system audit reports, cybersecurity audit reports, and any other reports required by SEBI CSCRF
- CSPs shall provide visibility to Skywards Investec and, when required, to SEBI, into CSP's infrastructure and compliance with applicable SEBI regulations
- Data stored with CSPs must reside on servers within India (data localisation); routing through servers outside India without SEBI approval violates data sovereignty expectations
- Encryption keys and their management shall remain within India and under Skywards Investec's control
- Skywards Investec shall conduct regular audits and VAPT of its cloud deployments.

A8. Pillar 7 — Audits, VAPT & Compliance Reporting

A8.1 Cyber Audit

Requirement	Details
Auditor	Only CERT-In empanelled cybersecurity auditors are permitted to conduct the cyber audit
Frequency	Qualified REs and MIIs: twice a year (half-yearly). Mid-size and Small-size REs: at least once a year. (Exact frequency determined by Skywards Investec's category)
Audit Period	Cyber audit for the period April 2025–March 2026 shall begin after March 2026. REs may follow CSCRF or previously issued SEBI circulars for the April 2024–March 2025 period.
Report Submission	Cyber Audit report shall be submitted to the relevant Stock Exchange within 1 month of completion of the audit
Format	Cyber Audit report must follow the Structured Format specified in Annexure-B of SEBI CSCRF
CEO Declaration	A compliance declaration/certificate signed by the MD/CEO/Partner/Proprietor shall accompany the audit report, certifying compliance with SEBI CSCRF

A8.2 Vulnerability Assessment & Penetration Testing (VAPT)

- VAPT shall be conducted by a CERT-In empanelled security firm to detect vulnerabilities in all critical systems, infrastructure components, and IT systems as defined in SEBI CSCRF.

- Frequency: Qualified REs — twice a year; Mid/Small-size REs — at least once a year; VAPT is also mandatory after every major release of the Bullsmart platform and after any major system change
- VAPT shall follow industry standards including OWASP and SANS guidelines, covering application layer, network layer, infrastructure, APIs, and business logic
- Critical vulnerabilities identified: must be remediated within 24 hours; High severity: within 7 days; Medium: within 30 days
- VAPT report shall be submitted to the relevant Stock Exchange within 1 month of completion of VAPT activity, in the SEBI CSCRF prescribed Annexure-A format
- Virtual patching may be used as a temporary measure while OEM patches are awaited, subject to CERT-In guidelines and OEM confirmation

A8.3 Red Teaming (Qualified REs & MIIIs)

- MIIIs and Qualified REs are mandated to conduct Red Teaming exercises as part of their cybersecurity framework
- Red Teaming is defined as a simulated adversarial exercise conducted under real-world conditions to comprehensively assess the security capabilities of the organisation and its systems
- Red Team exercises shall be planned, documented, and the findings addressed through remediation plans reviewed by the IT Committee

A8.4 ISO 27001 Certification

- ISO 27001 certification (latest version) is mandatory for MIIIs and Qualified REs as per SEBI CSCRF
- Skywards Investec shall obtain ISO 27001 certification if it falls in the Qualified RE category; deadline: August 20, 2025
- ISO 27001 provides essential security standards for the Information Security Management System (ISMS) that underpins this Policy

PART B — INVESTOR PHISHING & CYBER FRAUD AWARENESS ADVISORY

B1. Message to Our Investors

Dear Valued Client,

At Skywards Investec Private Limited, the safety of your investments and digital assets is our highest priority. As India's digital financial ecosystem grows rapidly, so does the sophistication of fraudsters who seek to exploit investors. SEBI has reported a 175% surge in phishing attacks within the BFSI sector in 2024, with over 135,000 phishing incidents recorded in the first half of 2024 alone.

In July 2025, SEBI, NSE, BSE, CDSL, NSDL, MCX, and AMFI jointly launched the 'SEBI vs SCAM' campaign to educate investors about digital fraud. This Advisory is published as part of Skywards Investec's investor protection obligations under SEBI CSCRF and our own commitment to your security. Please read this carefully and share it with family members who invest.

B2. Types of Cyber Fraud Targeting Investors

Sr. No.	Fraud Type	How It Works
1	Phishing Emails / SMS	Fake messages appearing to be from Bullsmart, SEBI, or exchanges — containing malicious links requesting OTPs, passwords, or demat credentials
2	Fake Trading Apps	Fraudulent apps mimicking the Bullsmart app on unofficial download links; investors deposit money and lose it permanently
3	Fake Websites	URLs nearly identical to www.bullsmart.in (e.g., bullsmart.co.in , bull-smart.com) designed to steal login credentials
4	SEBI Impersonation	Forged SEBI/NSE/BSE letterheads demanding payment of 'penalties' or 'compliance fees' — SEBI never does this
5	Social Media Scams	Fake Telegram groups, WhatsApp communities, YouTube channels impersonating Bullsmart or SEBI officials promising guaranteed returns
6	Deepfake / AI Impersonation	AI-generated videos of SEBI officials or executives promoting fraudulent schemes
7	Account Handling Scams	Offers to 'manage' your trading account requiring you to share login credentials — SEBI Press Release No. 14/2026
8	SIM Swap Fraud	Fraudsters obtain a duplicate SIM to intercept OTPs and take over trading accounts
9	Vishing (Voice Phishing)	Callers posing as Bullsmart support, SEBI officials, or banks asking for OTPs or passwords
10	KYC Fraud	Fake messages claiming KYC has expired and requesting credentials via unofficial links

B3. Investor Dos & Don'ts — Your Cyber Safety Checklist

B3.1 Protect your Bullsmart account by following these steps at all times

- Download the Bullsmart app ONLY from the official Google Play Store or Apple App Store — search 'Bullsmart by Skywards Investec'
- Access the Bullsmart web portal ONLY via www.bullsmart.in — verify the URL and HTTPS padlock before entering credentials
- Keep your Password, MPIN, TPIN, and OTP strictly confidential — never share them with anyone including family members
- Log out of the Bullsmart App after every trading session, especially on shared devices
- Verify sender email addresses — all official Bullsmart emails come ONLY from @bullsmart.in or @skywardsinvestec.com
- Transfer funds only through the Bullsmart App's in-built fund transfer feature — to your own registered bank account
- Verify the SEBI registration of any investment entity before investing: sebi.gov.in → Intermediaries
- Enable biometric authentication (fingerprint / Face ID) on the Bullsmart App for additional security
- Check your account transaction history regularly for any unauthorised trades or fund movements
- Report suspicious activity immediately to cybersecurity@bullsmart.in and call our helpline.

B3.2 The following should not be followed for securing the Bullsmart account from exactly what fraudsters count on:

- Never share your Password, OTP, TPIN, or MPIN with anyone — including anyone claiming to be from Bullsmart, SEBI, NSE, or BSE
- Never click links in SMS or WhatsApp messages claiming to be from Bullsmart or SEBI — unless independently verified
- Never download the Bullsmart app from links received in SMS, WhatsApp, or email — only from official app stores
- Never transfer money to any individual's personal bank account or UPI ID for investment or trading
- Never install screen-sharing or remote-access apps (AnyDesk, TeamViewer) on a caller's request
- Never invest based on tips from WhatsApp groups, Telegram channels, YouTube videos, or unverified social media
- Never share your trading credentials with 'account managers' offering to generate profits on your behalf
- Never panic at urgent messages about 'account blocked', 'legal action in 24 hours' — these are scare tactics

- Never trust 'SEBI officials' or 'fund managers' met online demanding payment into a bank account
- Never access Bullsmart on public Wi-Fi or jailbroken/rooted devices

B.4 How Skywards Investec Will and Will Never Contact You

Bullsmart WILL	Bullsmart will NEVER
Send communications from @bullsmart.in or @skywardsinvestec.com only	Ask for your Password, OTP, TPIN, or MPIN by any means
Send OTPs to your registered mobile AND email simultaneously	Request you to download the app from a WhatsApp or SMS link
Alert you for every login event via SMS and email	Ask you to transfer money to any individual's bank or UPI.
Send ECNs within 24 hours of every trade to your registered email	Offer guaranteed returns, risk-free profits, or hot stock tips
Address you by your registered name in all official communications	Contact you through WhatsApp, Telegram, or Instagram for services
Direct you to SEBI SCORES for any regulatory complaint	Ask you to join a premium group, VIP channel, or pay for advice
Always identify as a SEBI-registered entity with our registration number	Ask you to install screen-sharing or remote access software
Process fund transfers only to your own registered bank account	Impersonate SEBI officials or demand penalty payments

B5. Immediate Action Steps If You Suspect Fraud

Step	Action	How/Where
1	Change Bullsmart Password Now	Bullsmart App → Settings → Security → Change Password. Also change MPIN and TPIN immediately.
2	Freeze Your Account	Call Skywards Investec helpline immediately to request account suspension.
3	Report to Bullsmart	Email: cybersecurity@bullsmart.in Include your client ID and details of the fraud.
4	Report to SEBI SCORES	https://scores.sebi.gov.in Toll-Free: 1800 22 7575 / 1800 266 7575
5	Report to Cyber Crime Portal	https://cybercrime.gov.in Helpline: 1930 (24x7 National Cyber Crime Helpline)
6	File a Police FIR	At nearest police station or state's online FIR portal
7	Report Fake Sites/Apps to CERT-In	incident@cert-in.org.in — India's national cybersecurity agency

8	Inform Your Bank	If bank fraud occurred, contact your bank immediately to block transactions
9	Preserve All Evidence	Save all communications — emails, SMS, WhatsApp screenshots. Do NOT delete anything.

B6. Official Contacts — Quick Reference

Authority	Contact	Purpose
Bullsmart Cybersecurity Team	cybersecurity@bullsmart.in	Report fraud & account compromise
Bullsmart Customer Support	support@bullsmart.in App → Help & Support (24x7)	General platform queries
Bullsmart Grievance Officer	grievance@bullsmart.in	Formal complaints
SEBI SCORES 2.0	scores.sebi.gov.in	Complaints against SEBI-regulated intermediaries
National Cyber Crime Portal	cybercrime.gov.in 1930 (24x7 Helpline)	Report cyber fraud, phishing
CERT-In	incident@cert-in.org.in cert-in.org.in	Report phishing sites, malware, cyber incidents
NSE Investor Service Centre	investorservice@nse.co.in	NSE-related trade/broker complaints
BSE Investor Service Centre	is@bseindia.com	BSE-related trade/broker complaints
SEBI Official Website	www.sebi.gov.in	Verify registrations, SEBI enforcement actions

STAY VIGILANT. STAY SAFE. TRADE SMART. — SKYWARDS INVESTEC PRIVATE LIMITED | BULLSMART

Skywards Investec Private Limited | compliance@bullsmart.in | www.bullsmart.in | SEBI Reg: INZ000315235
Report cyber fraud: cybersecurity@bullsmart.in | National Cyber Crime: 1930 | SEBI Helpline: 1800 22 7575