Policy on Prevention of Impersonation and Unauthorised Use of Name & Logo

1. Policy Objective

This policy sets out a framework to identify, mitigate, and address risks arising from the impersonation of Spread X Securities Private Limited ("the Company") and the unauthorised use of its name/logo in the market, primarily in digital and social media spaces. The policy also outlines proactive steps for client awareness and regulatory compliance.

2. Scope

Applies to all employees, authorised persons (APs), business partners, and any entity acting on behalf of the Company.

3. Roles and Responsibilities

- **Compliance Officer**: Overall owner of the policy, responsible for ensuring implementation and reporting.
- **IT/Social Media Team**: Responsible for regular online monitoring and action against unauthorised use.
- **Client Servicing/Grievance Redressal**: Responsible for client communications and awareness initiatives.
- **HR & Admin**: To assist in internal investigations involving staff or APs.

4. Implementation Mechanism

4.1. Social Media & Online Surveillance

- Conduct fortnightly reviews of key social media platforms, web portals, and messaging apps for any unauthorised usage of the Company's name/logo or fraudulent claims of association.
- Maintain a log of all such reviews and findings for audit and compliance verification.

4.2. Detection & Response Protocol

- On identification of impersonation, scam promotion, or misrepresentation:
- Record all evidence (screenshots, URLs, communication logs).
- File a formal complaint with the concerned platform (social media, website host, messaging service).
- File a police complaint under relevant cybercrime provisions.
- Maintain records of all complaints lodged and their status.

4.3. Regulator & Stakeholder Notification

- Report all such incidents to the Stock Exchanges via official communication channels within three (3) days of police complaint filing, as per circular requirements.
- Provide detailed status updates on action taken and correspondence with authorities.

4.4. Client & Public Awareness

- Issue regular advisories/caution notices via the Company website, emails, SMS, and official social media handles, warning about such schemes and advising clients to verify communications through official channels only.

- Clearly display information on the Company's genuine accounts, website, and helplines.

4.5. Employee & Partner Vetting

- Investigate whether any internal employee, AP, or business partner is involved in reported impersonation.
- Take disciplinary action as per Company policy if involvement is established.

4.6. Documentation & Record-Keeping

- Maintain proper documentation of all monitoring activities, reports, complaints, and action taken.
- Retain records for a minimum of 8 years or as mandated by regulation.

5. Training & Awareness

- Conduct periodic employee training on identifying and reporting unauthorised activities.
- Incorporate guidelines into onboarding material for new joiners and APs.

****