# ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

## PROCEDURES FOR REPORTING UNUSUAL ACTIVITIES

| | |
|---|---|
| **Version** | **2024/01.02** |
| **Review Date** | **05/04/2024** |
| **Review & Approved by** | **Reviewed by Technology Committee & Approved by Board of Directors** |

**1. Introduction:**

This policy outlines the roles, responsibilities, and plan of action for dealing with DoS and DDoS attacks within the Organization, which operates as a stock broker and depository participant. The purpose of this policy is to establish a framework for effective incident response, ensuring the continued availability and security of our services.

**2. Roles and Responsibilities:**

**a.** Incident Response Team:

- ➤ Designate a team consisting of representatives from IT, network security, operations, and management.
- ➤ Appoint an incident response team leader responsible for coordinating the response efforts during an attack.
- ➤ Define the responsibilities of each team member, including incident detection, analysis, mitigation, communication, and documentation.

**b.** IT and Network Security Staff:

- ➤ Monitor network traffic and system logs to identify potential DoS/DDoS attacks.
- ➤ Implement appropriate security measures, such as firewalls, intrusion detection systems (IDS), and traffic filtering.
- ➤ Coordinate with the incident response team to initiate mitigation strategies.

**c.** Operations Staff:

- ➤ Collaborate with the incident response team to assess the impact of an attack on trading and depository services.
- ➤ Follow incident response procedures for containment, recovery, and service restoration.

**3. Incident Response Plan:**

**a.** Detection and Response:

- ➤ Deploy intrusion detection and prevention systems to detect and alert potential DoS/DDoS attacks.
- ➤ Establish monitoring thresholds and alerts for abnormal network behaviour.
- ➤ Define procedures for immediate response, including isolating affected systems or services, activating the incident response team, and notifying management.

**b.** Analysis and Mitigation:

- ➤ Investigate the nature and scale of the attack to determine if it is a DoS or DDoS attack.
- ➤ Engage network security staff to implement appropriate mitigation techniques, such as rate limiting, traffic filtering, or traffic diversion.
- ➤ Continuously monitor the effectiveness of mitigation measures and adjust as necessary.

**c.** Communication and Reporting:

- ➤ Establish communication channels within the incident response team and with relevant stakeholders.
- ➤ Notify management, regulatory authorities, and clients as necessary, providing updates on the incident, impact, and progress of mitigation efforts.
- ➤ Prepare incident reports detailing the attack, response actions, and lessons learned for future improvement.

**4. Review and Improvement:**

This policy will be reviewed annually to ensure its effectiveness, considering changes in technology, emerging threats, and industry best practices. Lessons learned from previous incidents and regular training exercises will be used to enhance response capabilities and strengthen the organization's resilience against DoS/DDoS attacks.

By adhering to this policy, Member aims to safeguard its trading and depository services, maintain business continuity, and protect the interests of its clients and stakeholders in the face of DoS and DDoS attacks.