NEON VINIMAY PVT. LTD.
Regd. Office : 510, Kamalalaya Centre, 156-A Lenin Sarani, Kolkata - 700 013
Phone : (033) 4062-7201 to 7213, CIN : U51109WB1993PTC057361
E.mail : backoffice@neonvinimay.com, neonvinimay04@gmail.com

STANDARD OPERATING PROCEDURE (SOP) FOR HANDLING CYBER SECURITY INCIDENTS

The Company is to follow the below-mentioned SOP for handling of Cyber Security Incidents which has been approved the Board of Directors in its Meeting on 05/06/2023

1. Introduction

This document outlines the Standard Operating Procedure (SOP) for handling cyber security incidents in accordance with the directives of the Securities and Exchange Board of India (SEBI) for intermediaries, specifically for a stock broker firm. The SOP defines the process for classifying and responding to cyber security incidents, reporting incidents to relevant authorities, and submitting necessary details to the Exchange and SEBI. This SOP have been approved by the Board of the Member, Partners, or Proprietor) and reviewed annually by the Internal Technology Committee as per SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, for the review of Security and Cyber Resilience policy.

2. Cyber Security Incident Classification

Cyber security incidents shall be classified into three categories based on their severity:

a. High: Incidents with significant impact, posing a severe threat to the firm's systems, data, or operations.

b. Medium: Incidents with moderate impact, causing disruption but not resulting in severe damage or compromise.

c. Low: Incidents with minimal impact, resulting in minor disruptions or unauthorized access attempts.

- All the incidents falling under the under-mentioned category shall be classified as a High Risk Incident irrespective of the fact whether they are intentional or unintentional:

- Incidents that have financial implication;
- Incidents that will /might have any impact on confidential organization data;

Regd. Office : 510, Kamalalaya Centre, 156-A Lenin Sarani, Kolkata - 700 013
Phone : (033) 4062-7201 to 7213, CIN : U51109WB1993PTC057361
E.mail : backoffice@neonvinimay.com, neonvinimay04@gmail.com

- Incidents that have resulted into any kind of compromise of critical data like user ids, passwords, admin rights, unauthorized access etc;

- Any kind of virus, malware, ransom ware attacks effecting the information system.

It is to be ensured that any kind of cyber security incident as mentioned in our Cyber Security and Resilience Policy shall be by default classified as a High Risk Incident. The degradation of these incidents into Medium / Low Risk Category shall be backed by sufficient recorded evidences along with the approval of Chief Information Security Officer (CISO) / Designated Officer (DO) / Members of Internal Technology Committee (MITC).

3. Incident Response Decision

The Cyber Security incident handling process document shall define the appropriate action/response for each category of incident. The response should be based on the severity of the incident and may include but is not limited to the following actions:

a. High: Promptly isolate affected systems, conduct forensic analysis, notify relevant stakeholders, escalate to the designated authorities, implement containment measures, and restore systems and data.
b. Medium: Assess the impact, investigate the incident, contain and mitigate any potential threats, notify relevant stakeholders, and take necessary corrective actions.

c. Low: Assess the incident, monitor for any escalation, take appropriate steps to prevent further compromise, and document the incident for future reference.

4. Reporting to CERT-In

Members shall report all cyber security incidents to the Indian Computer Emergency Response Team (CERT-In). The following steps shall be followed:

a. Provide a detailed report of the incident to CERT-In.
b. Share the reference details of the reported incident with CERT-In to the Exchange and SEBI.
c. Communicate with CERT-In for any required assistance regarding the reported incident.
d. If the incident is not reported to CERT-In, provide the reasons for not doing so to the Exchange and SEBI.

5. Communication with Relevant Authorities

NEON VINIMAY PVT. LTD. KOL.

Regd. Office : 510, Kamalalaya Centre, 156-A Lenin Sarani, Kolkata - 700 013
Phone : (033) 4062-7201 to 7213, CIN : U51109WB1993PTC057361
E.mail : backoffice@neonvinimay.com, neonvinimay04@gmail.com

Members shall engage with relevant authorities to seek further assistance and take appropriate actions in response to the cyber security incident:

a. Communicate with CERT-In, Ministry of Home Affairs (MHA), or the Cyber Security Cell of the Police for additional support and guidance.
b. Register the incident as a complaint with law enforcement agencies such as the Police or its Cyber Security cell if necessary.
c. Provide details of the reported incident and any actions taken to the Exchange and SEBI.
d. If a complaint is not registered, provide the reasons for not doing so to the Exchange and SEBI.

6. Reporting to Division Chiefs and CISO of SEBI

Members shall submit the details of the reported cyber security incident and the submissions made to various agencies to the Division Chiefs (in-charge of divisions at the time of submission) of the Department of Supervision-Market Intermediaries Regulation and Supervision Department (DOS-MIRSD), as well as the Chief Information Security Officer (CISO) of SEBI.

7. Ongoing Reporting Obligations

The Designated Officer of the Member, appointed as per para 6 of the aforementioned SEBI Circular dated December 03, 2018, shall:

a. Report any unusual activities and events within 6 hours of receiving such information.
b. Submit a quarterly report on cyber-attacks and threats within 15 days after the end of each quarter. The report should be submitted as specified in the Exchange's circular.

8. Review and Approval

This SOP for Cyber Security Incident Handling shall be reviewed annually by the Internal Technology Committee and approved by the appropriate authority (Board of the Member, Partners, or Proprietor) as required.

Note: The Designated Officer shall continue to report any unusual activities and events within 24 hours of receipt of such Information as well as submit the quarterly report on the cyber-attacks & threats within 15 days after the end of the respective quarter or in any other manner as specified by the Regulator from time to time.

For NEON VINIMAY PVT. LTD.

DIRECTOR