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

Data Requirement – Cyber Security Audit

1. POLICY DOCUMENT

1.1. Kindly provide comprehensive updated Cyber Security and Cyber Resilience policy document as per SEBI Circular - SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018 along with the Board Resolution for latest updated policy adopted.

1.2. Kindly provide the details of the Internal Technology Committee comprising of experts. Such Committee should on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board, and such review should include review of their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience. Kindly provide minutes of the last meeting of the Technology Committee.

1.3. Kindly provide the detailed and defined roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Their reporting and compliance requirements shall be clearly specified in the security policy. In addition, please also share the details of CISO with CERT-In through Email (info@cert-in.org.in)

1.4. Policy to handle technical glitches along with the board resolution for approval of the policy.

1.5. Policy for handling social media access along with the board resolution for approval of the policy.

2. ASSET DETAILS

2.1 List of all IT related Assets (Hardware and Software). Refer Asset List Format. **All columns are to be filled for each asset in Assets Register.**

2.2 Kindly provide the network diagram.

3. DATA PROTECTION

3.1 Access Control

3.1.1 Total user list of Trading Application (NEAT, ODIN, BEST etc) during the Audit Period including user details, user rights, location, IP address, certifications etc. In case of Exchange provided trading applications, kindly provide this data from the Exchange Interface. In case of in-house / third party trading application this data is to be obtained from respective server. Kindly also provide the date upto which individual user access is provided.

3.1.2 Details of personnel to whom Admin / Privilege access of respective databases are provided along with their designations. Kindly provide activity logs of such users.

3.1.3 Password Policy of respective servers and databases including minimum length, password complexity, password encryption, password history, max password age, account lockout duration. Provide screenshots. Declaration of removal of default password from devices and strong password implementation.

3.1.4 List of resigned employees during the audit period along with their last working date and the date of deactivation of their user rights and physical access. Access Register to be maintained with Expiry date of Access.

3.1.5 Declaration that no person by virtue or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

3.2 Physical Security

3.2.1 List of all Employees including Dealers, Outsourced Staffs, Vendors etc

3.2.2 List of officials having physical access to critical systems (Network Room, Server Room, Trading Floor etc). Maintenance of Visitor Registers.

3.3 Network Security Management

3.3.1 LAN and Wireless Network should be secured, Supporting to substantiate the regular update of all the software.

3.3.2 Supporting to substantiate Firewall status of Operating systems.

3.3.3 Supporting to substantiate firewall, malware, ransomware status of Anti Virus Software.

3.4 Data Security

3.4.1 Details sent to clients over e-mails should be password protected and critical details like Bank Account Numbers, Mobile Numbers etc should be masked.

3.4.2 Data Backup Policy of the organization including the storage facility and frequency of Back-up of critical data.

3.4.3 Whether any strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) are used to prevent Man-In-The-Middle (MITM) attacks during data transfer.

3.4.4 Kindly provide list of all open ports whether in use or not.

3.5 Application Security in Customer Facing Applications

3.5.1 Supporting to substantiate that applications such as IBTs, SWSTs, Back office etc. over the Internet are password protected. In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory. In case of Applications installed on mobile devices a secure biometric two-factor authentication mechanism may be used.

3.5.2 In case IBT / SWST / Mobile Trading are offered to clients, kindly provide logs of successful and failed login attempts against client's account.

3.5.3 Supporting to substantiate the prohibition of usage of unauthorized storage devices (like blocking of USB Drives, CD ROMs etc) on the systems containing critical information.

3.6 Certification of Off-the-Shelf Products

Kindly provide the requisite certifications form the vendors of off the shelf products used by you for core business functionality such as Back office applications and STQC certificate.

3.7 Patch management

3.7.1 Kindly confirm whether the new patches of critical software are tested before implementation.

3.7.2 Kindly provide latest VAPT Assessment Report.

4. MONITORING AND DETECTION

4.1 Kindly provide details of all the below-mentioned events (if any) during the audit period-
Security events / alerts, detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties.

4.2 Wherever incidents have been generated, please provide the tracking and closing of such incidents.

5. RESPONSE AND RECOVERY OF DATA

5.1 Kindly provide the Response and Recovery Plans for the timely restoration of systems affected by incidents of cyber-attacks including the responsibilities of employees and support staff in the event of cyber-attacks.

5.2 In case of any data destruction during the audit period, kindly provide the incident logs and learnings from such incidents.

5.3 Kindly provide details of data recovery drills conducted during the audit period along with the Data Backup Policy.

5.4 Kindly provide the details of Disaster Recovery Site, if any.

6. SHARING OF INFORMATION

6.1. Kindly provide details including dates on which Quarterly Reports were submitted to the Exchanges / Depositaries during the Audit period.
6.2. Kindly provide details of report submitted to Stock Exchange regarding Software as a service (SaaS) Based Solutions (as per SEBI circular dated November 3, 2020)

7. TRAINING AND EDUCATION

7.1 Kindly provide the details of Cyber Security Training Programs conducted during the audit period along with attendees and program curriculum. (Any 2 programs during the audit period).

7.2 Kindly provide the details of training provided to the employees to avoid clicking on a link in a spear-phishing email, reusing their personal password on a work account, mixing personal with work email and/or work documents, or allowing someone they shouldn't to use their corporate device- especially in Work from Home environments.

8. SYSTEMS MANAGED BY VENDORS

Kindly provide instructions issued to vendors (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications to ensure compliance with the policy guidelines.

9. MISCELLANEOUS DETAILS

9.1 Stockbrokers / Depository Participants should Enforce BYOD (Bring your own device) security policies, like requiring all devices to use a business-grade VPN service and antivirus protection. Kindly confirm such limitations. Register for BYOD devices with employee name and confirmation.

9.2 The stock brokers should formulate Standard Operating Procedure and adhere with the SOP for handling and reporting of Cyber Security Incidents. The aspects which shall form part of the SOP and which needs to be complied with by stock Brokers should be as per Exchange circular NSE/INSP/48163 dated May 03, 2021.

9.3 Service Level Agreements (SLA) & Non-Disclosure Agreements (NDA) with vendors.

10. DECLARATIONS

10.1. Declaration if there is no incident of technical glitches during the period. Else, give details & report submitted to exchange quarterly.
10.2. Declaration of LAN and WAN security. WAN to be password controlled
10.3. Declaration of any incident reported for CERTIN and Cyber Cell of Police.
10.4. Declaration for isolation of Algo servers of third party report of vendors safety and security
10.5. Declaration for non-removal /disposal of any devices during the period if remove then all protocol followed.
10.6 Declaration confirming compliance with the advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions issued by the Indian Computer Emergency Response Team (CERT-in) as per SEBI Circular no. SEBI/HO/MIRSD2/DOR/CIR/P/2020/221 dated November 03, 2020 - The compliance of the advisory shall be reported in the half yearly report by to stock exchange / depository participants with an undertaking).

11. OTHER REPORTS

11.1 Nessus Report of all network devices, firewall and all systems with action taken report and compliance status.
11.2 VAPT Report from CERTIN empanelled vendor.
11.3 Report on bandwidth usage-monthly report / screen shot of critical system or servers
11.4 Quarterly intimation to the Stock Exchange regarding use of AI and ML application and systems
11.5 Report on Mock Phishing Drills
11.6 Backup logs such as user access logs, event log / firewall reports for two (2) years.

PART OF ONSITE VERIFICATION

NEON VINIMAY PVT. LTD.

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

Screenshot of each PC/Laptop for the following:

- **How to verify Windows Registered Version** - Click on Start, then Control Panel, then click on System and Security, and finally click on System. Then scroll all the way down to the bottom and you should see a section called Windows activation, which says "Windows is activated" and gives you the Product ID.
- **How to verify Antivirus** - Click on Antivirus Icon on the bottom right hand side of the screen. Provide the screenshot of Antivirus Implementation and their enablement status.
- **How to verify OS Password Policy** - Click on Start- Control Panel- System & Security- Administrative Tools- Local Security Policy (click Open on top left)- Click on Account Policy - Password Policy - Account Lockout Policy. Provide Screenshot of Both the Screen
- **How to verify Firewall Status of Windows** - Click on Start - Control Panel- Click on System & Security - Click on Windows Firewall- Check the status and provide screenshot.

Images / Short video of Server Room, Firewall Device, CCTV Cameras, Access Control Devices, Trading Terminals & Back-office Servers.

For NEON VINIMAY PVT. LT.

DIRECTOR