MOHANLAL HEMCHAND PVT LTD

Cyber Security & Cyber Resilience framework
(Ref: SEBI Circular No.SEBI/HO/MIRSD/CIR/PB/2018/147 dated 3rd December, 2018 and SEBI Circular No.SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated 7th June, 2022)

Governance

1. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, MOHANLAL HEMCHAND PVT LTD has formulated a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. This policy document will be put up to the Board of MOHANLAL HEMCHAND PVT LTD for its approval and will be reviewed by the Board at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

2. This Cyber Security Policy includes the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:
   a. 'Identify' critical IT assets and risks associated with such assets.
   b. 'Protect' assets by deploying suitable controls, tools and measures.
   c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
   d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
   e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.

3. As MOHANLAL HEMCHAND PVT LTD do not undertake trading through APIs based terminal, the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') are not considered.

4. As MOHANLAL HEMCHAND PVT LTD do not undertake trading through APIs based terminal, best practices from international standards like ISO 27001, COBIT 5, etc., are not considered.

5. MOHANLAL HEMCHAND PVT LTD shall designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.

6. The Board shall constitute an internal Technology Committee comprising of experts. This Technology Committee shall 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. The review shall be placed before the Board for appropriate action.

7. MOHANLAL HEMCHAND PVT LTD shall establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.

8. The Designated officer and the technology committee shall periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

9. MOHANLAL HEMCHAND PVT LTD shall define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks towards ensuring the goal of Cyber Security.

Identification

10. MOHANLAL HEMCHAND PVT LTD identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board shall approve the list of critical systems. To this end, MOHANLAL HEMCHAND PVT LTD shall maintain up-to date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

11. MOHANLAL HEMCHAND PVT LTD shall accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

Protection

<u>Access controls</u>

12. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

13. Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. MOHANLAL HEMCHAND PVT LTD shall grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

14. MOHANLAL HEMCHAND PVT LTD shall implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. Illustrative examples for this are given in Annexure C.

15. All critical systems accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)

16. MOHANLAL HEMCHAND PVT LTD shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.

17. MOHANLAL HEMCHAND PVT LTD shall deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to the critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

18. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

19. MOHANLAL HEMCHAND PVT LTD shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT infrastructure.

20. User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

21. Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees.

22. Physical access to the critical systems should be revoked immediately if the same is no longer required.

23. MOHANLAL HEMCHAND PVT LTD shall ensure that the perimeter of the critical equipment room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

24. MOHANLAL HEMCHAND PVT LTD shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the premises with proper access controls.

25. For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.

26. MOHANLAL HEMCHAND PVT LTD shall install appropriate network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

27. Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application-based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.

Data security

28. Critical data must be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B.

29. MOHANLAL HEMCHAND PVT LTD shall implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B.

30. The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.

31. MOHANLAL HEMCHAND PVT LTD shall allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.

Hardening of Hardware and Software

32. MOHANLAL HEMCHAND PVT LTD shall only deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.

33. Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.

Application Security in Customer Facing Applications

34. Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative

list of measures for ensuring security in such applications is provided in Annexure C.

Certification of off-the-shelf products

35. MOHANLAL HEMCHAND PVT LTD shall ensure that off the shelf products being used for core business functionality (such as Back office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardization Testing and Quality Certification (Ministry of Electronics and Information Technology). Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.

Patch management

36. MOHANLAL HEMCHAND PVT LTD shall establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.

37. MOHANLAL HEMCHAND PVT LTD shall perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of data, systems and storage devices

38. MOHANLAL HEMCHAND PVT LTD shall frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

39. MOHANLAL HEMCHAND PVT LTD shall formulate a data-disposal and data- retention policy to identify the value and lifetime of various parcels of data.

Vulnerability Assessment and Penetration Testing (VAPT)

40. MOHANLAL HEMCHAND PVT LTD shall carry out periodic Vulnerability Assessment and Penetration Tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

41. MOHANLAL HEMCHAND PVT LTD shall conduct VAPT by engaging CERT-In empaneled organizations at least once in a financial year. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of MOHANLAL HEMCHAND PVT LTD, within 1

month of completion of VAPT activity.

42. In addition, MOHANLAL HEMCHAND PVT LTD shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

43. Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report.

Monitoring and Detection

44. MOHANLAL HEMCHAND PVT LTD shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

45. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, MOHANLAL HEMCHAND PVT LTD shall implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.

Response and Recovery

46. Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

47. The response and recovery plan of the MOHANLAL HEMCHAND PVT LTD shall have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. MOHANLAL HEMCHAND PVT LTD shall have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time

48. The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.

49. Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

50. MOHANLAL HEMCHAND PVT LTD shall also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

Sharing of Information

51. Quarterly reports containing information on cyber-attacks and threats experienced and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other shall be submitted to Stock Exchanges / Depositories.

Training and Education

52. MOHANLAL HEMCHAND PVT LTD shall work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).MOHANLAL HEMCHAND PVT LTD shall conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.

53. The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Systems managed by vendors

54. Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) are managed by vendors and MOHANLAL HEMCHAND PVT LTD may not be able to implement some of the aforementioned guidelines directly, the MOHANLAL HEMCHAND PVT LTD shall instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

Systems managed by MIIs

55. Where applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE’s NOW, BSE’s BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not MOHANLAL HEMCHAND PVT LTD. MOHANLAL HEMCHAND PVT LTD is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

Periodic Audit

56. The Terms of Reference for the System Audit of Stock Brokers specified vide circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013, shall accordingly stand modified to include audit of implementation of the aforementioned areas. MOHANLAL HEMCHAND PVT LTD (as defined in CIR/MRD/DMS/34/2013 dated November 06, 2013) shall arrange to have their systems audited on an annual basis by a CERT-IN empaneled auditor or an independent CISA/CISM qualified auditor to check compliance with the above areas and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board within three months of the end of the financial year.

Annexure A

Illustrative Measures for Data Security on Customer Facing Applications

1. Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the Stock Broker. They should ideally be in discrete silos or DMZs.
4. Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.
5. Use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.
6. Ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access endpoints, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes increasingly difficult.

Annexure B

Illustrative Measures for Data Transport Security

1. When an Application transmitting sensitive data communicates over the Internet with the Stock Brokers' systems, it should be over a secure, encrypted channel to prevent Man- In-The-Middle (MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with the Stock Brokers' systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) should be used.
2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).
3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

Annexure C

Illustrative Measures for Application Authentication Security

1. Any Application offered by Stock Brokers to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as "Application" hereafter) over the Internet should be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) should be enforced. While it is difficult to quantify password "complexity", longer passphrases have more entropy and offer better security in general. Stock Brokers should attempt to educate Customers of these best practices.
2. Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.).

   In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of failed login attempts into Applications, the Customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer's registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by the Broker after verification of the Customer's identity etc.
6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.
7. Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.