CYBER SECURITY AND CYBER RESILIENCE POLICY

VARDHAMAN CAPITAL PVT LTD, herewith referred as VCPL , is the SEBI registered Stock Broker &Depository Participant. The under-mentioned cyber security and cyber resilience policy is created by the Compliance Officer and approved by the Board of Directors on 28/02/2023.

1. STATUTORY MANDATE

This framework is formed in accordance with the requirements of the SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated December 3, 2018.

2. OBJECTIVE OF THE FRAMEWORK

The objective of this framework is to provide robust cyber security and cyber resilience to the Stock brokers and depository participants to perform their significant functions in providing services to the holders of securities.

3. APPLICABILITY

Provisions of the said circular and framing of cyber security and cyber resilience are required to be complied by all Stock Brokers and Depository Participants registered with SEBI.

The policy has been considered, taken on record and approved by the board of directors of the company at their duly convened meeting held on 28/02/2023

4. SCOPE OF THE FRAMEWORK

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

With the view to strengthen and improve Cyber Security and Cyber Resilience framework, the board of directors of the company shall review this policy documents and implementation thereof at least once annually.

5. DESIGNATED OFFICERand **CHIEF INFORMATION SECURITY OFFICER (CISO)**

The company nominates Anup Kumar Khandelwal as Designated Officer and Chief Information Security Officer of the company 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. CONSTITUTION OF TECHNOLOGY COMMITTEE

6.1 The company constitutes a technology committee ("the committee") with following members:

Sr. No. Name of the Committee Members Designation of the Members

1. Anup Kumar Khandelwal. 2. Shashi Chandra Mallah.
2. Brijesh Upadhyay. 3. Sanjay Kumar Tiwari.

6.2 Such committee shall on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy. Such review shall include but not limited upto, reviewing of current IT and Cyber Security and Cyber Resilience capabilities, setting up of goals for a target level of Cyber Resilience, and establishing plans to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board of directors for taking appropriate action(s), if required.
6.3 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.

7. IDENTIFICATION, ASSESSMENT AND MANAGEMENT OF CYBER SECURITY RISK

The company shall ensure the following steps in order to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems.

7.1 IDENTIFICATION OF CRITICAL IT ASSETS AND RISKS ASSOCIATED WITH SUCH ASSETS

The committee and designated officer shall identify the critical assets based on their sensitivity and criticality for business operations, services and data management including various servers, data processing systems, and information technology (IT) related hardware and software etc.
The IT team shall maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

7.2 PROTECTION OF ASSETS BY DEPLOYING SUITABLE CONTROLS, TOOLS AND MEASURES

In order to protect the cyber safety, the company shall ensure the measures which include, however not limited upto:

- Access controls
- Physical Security
- Network Security Management
- Data security
- Hardening of Hardware and Software
- Application Security in Customer Facing Applications
- Certification of off-the-shelf products
- Patch management
- Disposal of data, systems and storage devices
- Vulnerability Assessment and Penetration Testing (VAPT)

The company shall take all such steps to protect assets of the company by deploying suitable controls, tools and measures in conformity with the provisions of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018 and any amendment or substitution thereof. However, the committee and designated officer of the company shall additionally deploy such measures in this respect, as may be warranted from time to time.

7.3 DETECTION OF INCIDENTS, ANOMALIES AND ATTACKS THROUGH APPROPRIATE MONITORING TOOLS/PROCESSES

Necessary steps as may be required to monitor and for early 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 shall be maintained, appreciated and taken care on.
The security logs of systems, applications and network devices exposed to the internet shall also be, from to time, monitored for anomalies, if any.
The company shall ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, and implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

7.4 RESPONDING BACK BY TAKING IMMEDIATE STEPS AFTER IDENTIFICATION OF THE INCIDENT, ANOMALY OR ATTACK

The alerts generated from monitoring and detection of systems 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.
In case of affection of systems by incidents of cyber-attacks or breaches, the company shall ensure timely restoration of the same in order to provide uninterrupted services. The committee and designated officer shall ensure to have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements.
With a view to providing quick responses to such cyber-attacks, the committee shall formulate a response plan defining 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. Such plan and any modification therein shall be circulated amongst all the employees and support / outsourced staff from time to time.

7.5 RECOVERY FROM INCIDENT(S) THROUGH INCIDENT MANAGEMENT AND OTHER APPROPRIATE RECOVERY MECHANISMS

The company shall take into account the outcomes of any incident of loss or destruction of data or systems and accordingly shall take precautionary measures to strengthen the security mechanism and improve recovery planning and processes.
Periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

8. The technology committee in accordance with the provisions of the said circular and formed hereinafter this framework, shall ensure that this framework considers 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') and subsequent revisions, if any, from time to time.

9. COMMUNICATION OF UNUSUAL ACTIVITIES AND EVENTS

IT team of the company under guidance of the committee shall monitor unusual activities and events and shall facilitate communication of the same to designated officer for necessary actions, as may be required.

10. RESPONSIBILITIES OF EMPLOYEES, MEMBERS AND PARTICIPANTS

In addition to the followings, the employees, members and participants shall be responsible for the duties and obligations as may be entrusted and communicated by the company / committee / designated officer from time to time.

To prevent the cyber-attacks, the employees, members and participants shall assist the company to mitigate cyber-attacks by adhering the followings:

- To attend the cyber safety and trainings programs as conducted by the company from time to time.
- To endure installation, usage and regular update of antivirus and antispyware software on computer used by them.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Keep your Wi-Fi network secured and hidden.
- To adhere limited employee access to data and information and limited authority to install software.
- Regularly change passwords.
- Do not use or attach unauthorised devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on computer or any financial data on any unauthentic website.
- To get your computer regularly scanned with anti-virus software.
- Do not release sensitive data of the organization.

Further the company shall ensure that:

- No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.
- Any access to the systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. The company 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 shall be for the period when the access is required and should be authorized using strong authentication mechanisms.
- All critical systems accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.), as far as possible.
- The Company shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes and such logs would be maintained and stored in a secure location for a time period not less than two (2) years.
- The Company shall be required to deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to company's critical systems. Such controls and measures shall inter-alia include restricting the number of privileged users, if any, 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.
- 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, shall be subject to stringent supervision, monitoring and access restrictions.
- User Management shall address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
- Physical access to the critical systems shall be restricted to minimum and only to authorized officials. Physical access of outsourced staff / visitors shall be properly supervised by ensuring at the minimum that outsourced staff / visitors are accompanied at all times by authorized employees.

Physical access to the critical systems shall be revoked immediately if the same is no longer required.
The Company will ensure that the perimeter of the critical equipment's room, if any, shall be 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.
The Company 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 shall be secured within the premises with proper access controls.
For algorithmic trading facilities whenever implemented, adequate measures will be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications, if any.
The Company shall install 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.
Adequate controls shall be deployed to address virus / malware / ransom ware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.
Critical data shall 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.
The Company shall implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It shall ensure that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
This security policy also covers 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.
The Company shall allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
The Company 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.
Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data shall be blocked and measures taken to secure them.
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 by Brokers to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. Required measures for ensuring security in such applications shall be ensured.
The Company shall ensure that off the shelf products, if any, 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) Standardisation 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 shall include business logic and security controls.

The Company 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.

The Company 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.

Suitable policy for disposal of storage media and systems shall be framed as may be required. The critical data / Information on such devices and systems shall be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

The Company shall formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.

The Company shall regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet, as and when required.

The Company with systems publicly available over the internet shall also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.

In addition, the company shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, the company shall report them to the vendors and the exchanges in a timely manner.

Remedial actions, if required, shall be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

The Company shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely 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. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies, if any.

Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, the company 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.

Alerts, if any, generated from monitoring and detection systems shall 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.

The response and recovery plan of the company 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. The company shall have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements.

Responsibilities and actions to be performed by company's employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism shall be defined.

Any incident of loss or destruction of data or systems shall be thoroughly analysed and lessons learned from such incidents shall be incorporated to strengthen the security mechanism and improve recovery planning and processes.
Suitable periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.
All Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents.
The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.
The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Stock Brokers / Depository Participants / Exchanges /Depositories and SEBI shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year. The above information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.
 Conducting VAPT at least once in a financial year by a CERT-In empaneled organization. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.
 Shall ensure that the Standard Operating Procedure (SOP) for handling Cyber Security incidents as specified by Exchange circulars from time to time are duly implemented.
 Any unusual activities and events should be reported by Designated Officer within 24 hours of receipt of such Information.

11. SUBMISSION OF QUARTERLY REPORTS

Quarterly reports containing information on cyber-attacks and threats experienced, if any, by the company and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants shall be submitted to Stock Exchanges / Depositories, as per statutory requirements / guidelines.

12. TRAINING AND EDUCATION

The committee and designated officer shall conduct training and educational sessions for employees to make them aware on building Cyber Security and basic system hygiene awareness, to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to date Cyber Security threat alerts, including to outsourced staff, vendors, if any, and shall take all such steps as may be deemed appropriate by them in this respect.

13. SYSTEMS MANAGED BY VENDORS

Whenever the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of the company are managed by vendors and the company may not be able to implement some of the aforementioned guidelines directly, the company shall, from time to time, 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.

14. SYSTEMS MANAGED BY MIIS

Wherever the 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 with the company. In such case, the company is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

15. INTERNET ACCESS POLICY

The Company shall ensure that the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the company's critical IT infrastructure shall be formulated.

16. PASSWORD POLICY

The Company shall follow strict password policy as prescribed by SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018. Any Application offered to Customers containing sensitive, private, or critical data over the Internet should be password protected. Wherever off the shelf products or third party products are used, respective vendors would be made aware regarding the implementation of a strict password policy as directed by SEBI circular. None of our In-house software, operating systems, servers, networks etc will be used with default passwords. Regular trainings will be conducted for our employees and staffs to make them aware regarding the importance of password confidentiality. The company will take strict action against anyone who breach the password policy. The clients will also be intimated from time to time regarding the importance of password confidentiality. Wherever possible, two-factor logins will be implemented.

17. DATA-DISPOSAL AND DATA-RETENTION POLICY

All critical data will be stored and retained in the secured manner as per the above mentioned mechanisms for such duration as may be required by various statutes from time to time. Critical data confidentiality is of utmost importance for the organisation and best efforts will be taken to ensure the same. Measures such as strong passwords, limited access, authenticated storage devices, regular back-ups etc will act as multiple protection layers in securing organisation's critical data. Once the retained data becomes redundant and time-barred, it will be disposed in a secured manner to ensure the avoidance of any misuse of organisation's data. Methods such as crypto shredding / degauss / Physical destruction will be used to dispose the redundant data.

18. PERIODIC AUDIT

The company shall arrange to have its systems audited on an annual basis by a CERT-IN empanelled auditor or an independent DISA / 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 / committee / any committee thereof within three months of the end of the financial year.

19. CONDUCTING VAPT TEST

The company shall ensure conducting VAPT test as per SEBI circular dated June 07, 2022 bearing reference number SEBI/HO/MIRSD/TPD/P/CIR/2022/80. The said circular states that every:

- Stock Brokers / Depository Participants shall 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/Partners/Proprietor of the Stock Brokers / Depository Participants shall approve the list of critical systems.
  To this end, Stock Brokers / Depository Participants 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.

- Stock Brokers / Depository Participants 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.

- Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity.
  In addition, Stock Brokers / Depository Participants 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.

Further, 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.

20. ADHERENCE TO CERT-IN ADVISORIES

In view of the rising incidents of data breaches / data leaks, CERT-In has issued an advisory dated January 20, 2021 with respect to "Preventing Data Breaches / Data Leaks". Our organisation shall adhere to the cyber security guidelines / advisories issued in the past and follow best industry practices and comply with other guidelines issued by CERT-In and NCIIPC from time to time.

21. PHASE-WISEIMPLEMENTATION OFCYBER SECURITY&RESILIENCE FRAMEWORK

Whereas it is evident that in the current scenario, Cyber Security and Cyber Resilience is of primary importance to any organisation. Our company will start implementing all the above-mentioned procedures and methodologies to ensure

cyber security and cyber resilience. With everyday increase in dependence on cyber environment, the risk of attacks are increasing day by day. Mere dynamic nature of cyber-attack is the main challenge in effective and efficient implementation of Cyber Security and Cyber Resilience mechanisms. While best efforts will be taken to implement all the steps and methods as mentioned in this policy in near future, we as an organisation strive to set new benchmarks in the industry by always staying one step ahead of malicious attackers. Whereas large number of systems as mentioned in this policy have already been implemented, we are in the process of adapting the remaining standards as soon as possible. Further this policy will be regularly reviewed to keep abreast with the ever-changing dynamic nature of cyber environment. Although implementing all the above steps attracts an exorbitant cost, the company intends not to make any compromise on Cyber Security and Cyber Resilience. Regular updates and suggestions by our peers, auditors, regulators and other intermediaries will not only help us in taking our implementation standards of Cyber Security and Cyber Resilience mechanism as per this policy but also to the Global Level.

22. CYBER SECURITY CONTROLS:

i. The Company shall deploy web and email filters on the network, configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages, scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
ii. The Company shall block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
iii. Restricting execution of "powershell" and "wscript" in enterprise environment, if not required. Ensuring installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. The Company shall send the associated logs to a centralized log repository for monitoring and analysis.
iv. Utilizing host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
v. Practice of whitelisting of ports based on business usage at Firewall level shall be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted shall be blocked by default.

23. SECURITY OF CLOUD SERVICES:

i. The Company shall check public accessibility of all cloud instances in use, make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
ii. The Company shall ensure proper security of cloud access tokens. The tokens shall not be exposed publicly in website source code, any configuration files etc.
iii. Implementing appropriate security measures for testing, staging and backup environments hosted on cloud. Ensuring that production environment is kept properly segregated from these. Disabling/removing older or testing environments if their usage is no longer required.
iv. The Company shall employ hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

24. CONCENTRATION RISK ON OUTSOURCED AGENCIES:

The Company shall take into account the concentration risk while outsourcing multiple critical services to the same vendor.

Enclosures:
Annexure A: Illustrative Measures for Data Security on Customer Facing Applications
Annexure B: Illustrative Measures for Data Transport Security
Annexure C: Illustrative Measures for Application Authentication Security

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 email 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.