CYBER SECURITY AND CYBER RESILIENCE POLICY

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.

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.

The policy document is approved by the Board of the Vardhamanglobal Sharecom Private Limited. 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. Governance

As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, We, Vardhamanglobal Sharecom Private Limited formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document.

The 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.

6. DESIGNATED OFFICER

The company has nominated a senior official or management personnel as Designated 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.

7. CONSTITUTION OF TECHNOLOGY COMMITTEE

7.1 The company constitutes has constituted internal technology committee comprising experts.

7.2 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.

7.3 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.

8. 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.

8.1 IDENTIFICATION
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.

8.2 PROTECTION
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.

Access Control

1. No person by virtue of rank or position have any intrinsic right to access confidential data, applications, system resources or facilities.
2. Any access to Vardhaman Sharecom Private Limited systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Vardhaman Sharecom Private Limited should 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.
3. Vardhaman Sharecom Private Limited 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.
4. All critical systems of the Vardhaman Sharecom Private Limited accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
5. Vardhaman Sharecom Private Limited ensures 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.
6. Vardhaman Sharecom Private Limited deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stock Broker/Depository Participant's 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.
7. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Vardhaman Sharecom Private Limited critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions
8. Vardhaman Sharecom Private Limited 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 Stock Broker/ Depository Participant's critical IT infrastructure.
9. 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

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

3. Stock Brokers/Depository Participants should ensure that the perimeter of the critical equipments room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards. CCTV card access systems, mantraps, bollards, etc., where appropriate.

Network Security Management
4. Vardhaman Sharecom Private Limited establish baseline standards to facilitate consistent application of security configurations to operating systems, databes, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the Stock Brokers/Depository Participants' premises with proper access controls.

5. For algorithmic trailing facilities, adequate measures should be taken to isolate and secure the perimeter and

connectivity to the servers running algorithmic trading applications

6. Vardhaman Sharecom Private Limited install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (ILS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

7. Adequate controls must 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.

Data security

1. 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.
2. Vardhaman Sharecom Private Limited 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.
3. 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.
4. Vardhaman Sharecom Private Limited allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
5. Hardening of Hardware and Software
6. Vardhaman Sharecom Private Limited 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
7. 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
1. 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. An illustrative list of measures for ensuring security in such applications is provided in Annexure C

Certification of off-the-shelf products
1. Vardhaman Sharecom Private Limited 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
1. 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

2. Vardhaman Sharecom Private Limited 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.

3. Vardhaman Sharecom Private Limited perform rigorous testing of security patches and updates, where I 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

1. Vardhaman Sharecom Private Limited 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.

2. Vardhaman Sharecom Private Limited 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)

1. Vardhaman Sharecom Private Limited regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet

2. Vardhaman Sharecom Private Limited 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 month of completion of VAPT activity.

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

4. Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing

8.3 Monitoring and Detection

Vardhamanglobal Sharecom Private Limited has established 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.

Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, Vardhamanglobal Sharecom Private Limited 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.

8.4 Response and Recovery

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.

The response and recovery plan of the Vardhamanglobal Sharecom Private Limited 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. Stock Brokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CAR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.
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.

The response plan 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.

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

Vardhamanglobal Sharecom Private Limited also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

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 unauthorized 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.

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.

All Cyber-attacks, threats, cyber-incidents and breaches experienced by Vardhamanglobal Sharecom Pvt Ltd shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.

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 Vardhamanglobal Sharecom Pvt Ltd, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

12. TRAINING AND EDUCATION
The committee and designated officer shall conduct periodic 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.

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

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. PERIODIC AUDIT

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

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. Analyze 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. Analyze 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 has 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.