Cyber Security Policy

1) Introduction -

An organization's Cyber Security and Cyber Resilience framework provides the safeguard from the:

a) 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).

b) Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience.

c) 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

Our Cyber Security and Cyber Resilience policy and framework cover the following areas of information security and controls as mandated by the SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018:

a) Governance

b) Identification

c) Protection

   I. Access controls
   II. Physical Security
   III. Network Security Management
   IV. Data security
   V. Hardening of Hardware and Software
   VI. Application Security in Customer Facing Applications
   VII. Certification of off-the-shelf products
   VIII. Patch management
   IX. Disposal of data, systems and storage devices

X. Vulnerability Assessment and Penetration Testing (VAPT)

d) Monitoring and Detection
e) Response and Recovery
f) Sharing of Information
g) Training and Education
h) Systems managed by vendors
i) Systems managed by MIIs
j) Periodic Audit

2) <u>Governance</u> -

a) The policy document approved by our Board and required to review this policy document at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

b) This policy documents Include the following process:

I. **'Identify'** critical IT assets and risks associated with such assets.
II. **'Protect'** assets by deploying suitable controls, tools and measures.
III. **'Detect'** incidents, anomalies and attacks through appropriate monitoring tools/processes.
IV. **'Respond'** by taking immediate steps after identification of the incident, anomaly or attack.
V. **'Recover'** from incident through incident management and other appropriate recovery mechanisms.

c) To implement the above framework, a Internal Technology Committee is formed comprising of following person:

1. Mr. <u>Merajuddin Md. Akbar</u> Information Technology Executive

2. Mr. <u>Niranjan Dhara</u> Compliance Officer

This Technology Committee required to **review on a half yearly basis** the implementation of the Cyber Security and Cyber Resilience policy approved by our Board, and also include review of our 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.

Technology Committee will also be responsible to placed result of such review before the Board for appropriate action.

Mr. Merajuddin Md. Akbar appointed as **Designated Officer** for the purpose of this policy, he will be responsible 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.

d) The Designated officer and the technology committee will also be responsible to periodically review the instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

e) We have also defined the responsibilities of our employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use our systems / networks towards ensuring the goal of Cyber Security.

3) Identification:

a) We have a system to identify critical assets based on their sensitivity and criticality for business operations, services and data management.

b) We have maintained up-to-date inventory of our 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.

c) We have a system to 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.

4) **<u>Protection</u>:**

a) **<u>Access Control</u>** -

I. We have not granted any intrinsic rights to any person by Virtue of rank or position to access our confidential data, applications, system resources or facilities.

II. Access granted for our systems, applications, networks, database, etc. only for a defined purpose and defined period and on a need to use basis and based on the principal of least privileges.

III. In our Access Policy, strong password controls defined for user's access to system, applications, networks and databases.

IV. We have inbuilt two-factor security (such as VPNs, Firewall Control, etc. in our all critical systems accessible over the internet.

V. We have maintained the records of our user access to critical system for audit and review purpose and retained such records for a minimum period of 2 years in a secured location.

VI. We deployed controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) of our 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 system logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

VII. In our internet access policy, monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within our critical IT infrastructure.

VIII. We have defined a system to deactivate the access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

b) Physical Security -

I. We have allowed physical access to our system only to authorized users. Outsourced staff /visitors are accompanied and supervised at all times by authorized employees at the time of physical access by them.

II. We have a system to revoke physical access to the critical system immediately is the same is no longer.

III. We 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.

c) Network Security Management

I. We have established baseline standards to facilitate the consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within our IT environment. The LAN and wireless networks are secured within our premises with proper access controls.

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

III. We have installed network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect our IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

IV. We have established adequate controls 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.

d) Data Security

I. We have identified and encrypted the data by using strong encryption methods.

II. We have implemented measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. Confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

III. Policy also covers the use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within our critical IT infrastructure, that can be used for capturing and transmission of sensitive data.

IV. We have allowed only authorized data storage devices within our IT infrastructure through appropriate validation processes

e) **Hardening of Hardware & Software**

I. We have 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.

II. We have blocked and measures taken to secure all open ports on networks and systems which are not in use or that can be potentially used for exploitation of data.

f) **Patch Management**

I. Patch management procedures include the identification, categorization and prioritization of patches and updates.

II. Performs rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches does not impact other systems.

g) **Disposal of data, systems and storage devices**

I. We have a 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.

II. We have also formulated a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.

h) Vulnerability Assessment and Penetration Testing (VAPT)

I. We have regularly conducted vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.

II. We have also carried out penetration tests with systems publicly accessible over the internet, 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.

III. In addition, we have also performed vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

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

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

5) Monitoring and Detection

a) We have 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 also monitored for anomalies.

b) Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, also implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

6) Response and Recovery

a) We have a system to investigate the alerts generated from monitoring and detection 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.

b) Our response and recovery plan ensure for the timely restoration of systems affected by incidents of cyber-attacks or breaches.

c) In case of any unforeseen incidents of loss or destruction of data or system, we will thoroughly analyze and lessons learned from any such incident and incorporated such result to strengthen the security mechanism and improve recovery planning and processes.

d) We conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

7) Sharing of Information

a) We will share information on cyber-attacks and threats experienced by us 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 on Quarterly basis and submitted to Stock Exchanges / Depositories.

8) **Training and Education**

a) We worked on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).

b) We 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.

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

9) **Systems managed by Vendors**

a) Our IBT, Back office and other Customer facing applications, IT infrastructure, etc. are managed by the vendors and we had already instructed our vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and we obtained the necessary self-certifications from them to ensure compliance with the policy guidelines.

10) **Periodic Audit**

a) We shall arrange to have our system audited on a periodic basis and shall obtain certification from any independent auditor, capable to do the same.