Cyber Security & Cyber Resilience Policy

Preface: Rapid technological developments in securities market have highlighted the need for maintaining robust cyber security and cyber resilience framework to protect the integrity of data and guard against breaches of privacy. Since stock broker and as depository participant perform significant functions in providing services to their clients, it is desirable that these entities have robust cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

Need of Policy:

Every stock broking entity as well as depository participant is required to Identify, assess and manage the Cyber Risks associated with processes, information, networks and systems.

Cyber Security Framework and Policy:

Ratnakar Securities Pvt Ltd shall follow below 5 Point framework for Cyber Security and Cyber Resilience Framework:

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

To implement the above framework, a Technology Committee shall be formed comprising of following individuals:

1.	Mr. Ajay Jayantilal Shah	Director
2.	Mr. Mayuri Ajay Shah	Director
3.	Mr. Sunil Thakker	Chief Information Security Officer (CISO)
4.	Mr. Kushal Ajay Shah	Compliance Officer

Designated Officer shall direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.

Identification: CISO shall identify all the critical assets based on their sensitivity and criticality for business operations and shall maintain an up to date inventory of its hardware and systems along with name and ID details of personnel to whom such hardware and systems are issued. He/she shall also be held responsible to identify the software installed, details of network, data flowchart and connection to the networks. The Board shall approve the list of critical systems.

CISO alongwith Designated Officer and external agencies (if required), shall identify the cyber risks that Ratnakar Securities Pvt Ltd may face alongwith the likelihood and impact of the same on business of company.

Protection:

No unauthorised person, irrespective of his/her designation, post or rank should have right to access critical systems, confidential data, applications or facilities.

Any access given shall be for defined period and defined purpose only. An access to IT systems, applications, databases and networks should be granted 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.

Any Application offered 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 minimum length of 6 characters of complex password shall be enforced across the applications. An attempt to educate the customers shall also be made by team.

Multi factor authentication (MFA) shall also be implemented across the applications in phased manner. Passwords, security PINs etc shall be stored in encrypted manner in one way hashed encryption using cryptographic hash functions.

After Three (3) 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, after verification of the customer's identity etc.

Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.

Ratnakar Securities Pvt Ltd shall also ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs shall be maintained for a period of minimum two years.

Ratnakar Securities 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.

IT team shall also address deactivation of access of privilege of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

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.

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

Perimeter of the critical equipment room (server Room)shall be secured physically 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

Continuous and consistent application of security configuration shall be made to Operating Systems, Databases, Network devices and enterprise mobile device with in the IT environment. The LAN and wireless network networks shall be secured with Firewall and Intruder Controller and continuous monitoring shall be made towards any attempt of unauthorised access to the network.

Every individual as well as network connected system shall have an Anti-Virus Software with Anti Malware and Anti Ransomware protection.

Data Security

All the critical data need to be identified and encrypted using strong encryption methodologies, such as masking of critical information, masking of passwords while logging in, encrypted transfer of password to server etc.

All the ports, for connecting external storage device or unauthorised USB tokens, of all critical systems as well as network connected systems shall be disabled and log shall be maintained for all the access granted for any given time to any users with specific reason of same.

Any authorised access to Printers, Scanner shall be prevented by application of proper access control and restricting the usage to prevent misuse of resources and to avoid transmission of sensitive data. Use of mobile phones shall not be allowed to any employees for dealing with clients as well as any other external parties and any call to clients shall be made using baseline phones having voice logger facility only.

Hardening of Hardware and Software

Procurement of all the hardware and software shall be done from renowned vendor/supplier only in company sealed packaging and any unauthorised software and hardware shall not be installed on any system, which form part of network. All the test software and hardware shall be installed and tested on designated separate system/network to prevent misuse from such devices and software.

Certification of off-the-shelf products

IT team shall ensure that all the off-the-shelf products procured for core business activities should bear Indian Common criteria certification of Evaluation Assurance Level 4 provided by STQC. 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

Team 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.

Team shall also 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.

All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching shall be considered for protecting systems and networks. However, patches should be sourced only from the authorized sites of the OEM.

Disposal of data, systems and storage devices

Any disposal of any data, system or storage devices shall be done in closely monitored manner. All the sensitive data, including encrypted system files, shall be removed completely before disposal of any system or storage device. The critical information on such devices shall be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

Designated Officer shall ensure regular conduct of 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.

Technology Committee shall ensure that vulnerability scanning and penetration testing is conducted prior to the commissioning of a new system which is a critical system or part of an existing critical system.

VAPT test shall be carried out atleast once in a year between Oct to Nov month by CERT-In empanelled organizations. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee within 1 month of completion of VAPT activity. Any gaps/vulnerabilities detected have to be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI/ Stock Exchange/ Depository within 3 months post the submission of final VAPT report.

The Designated Officer shall report the Cyber Security incident to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time.

The Designated Officer of the Member (appointed in terms of para 6 of the aforementioned SEBI Circular dated December 03, 2018) shall continue to report any unusual activities and events, all Cyber-attacks, threats, cyber-incidents and breaches experienced by Members to Exchange, Depository & SEBI (on the dedicated email ID sbdp-cyberincidents@sebi.gov.in) within 6 hours of noticing / detecting such incidents or being brought to the notice about such incidents as well as submit the quarterly reports containing the information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers 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 within 15 days after the end of the respective quarter in the manner as specified from time to time.

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

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

Monitoring and Detection

We 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.

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

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.

The response and recovery plan should 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. Team shall ensure that we have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions.

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

Sharing of Information

Quarterly reports containing information on cyber-attacks and threats experienced by our team 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.

Training and Education

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

We shall also 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. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email shall form part of training programs. Important highlights & updates of the advisories issued by CERT-In shall also be discussed in training programs.

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

Cybersecurity Controls & Security of Cloud Services

Following cybersecurity controls shall be introduced:

i. Deploy web and email filters on the network: We shall configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. We shall scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

ii. Block the malicious domains/IPs after diligently verifying them without impacting the operations. IT team shall refer CSIRT-Fin/CERT-In advisories which are published periodically for latest malicious domains/IPs, C&C DNS and links.

iii. Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. We shall ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled.

iv. Utilize 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 should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.

vi. Check public accessibility of all cloud instances in use. IT Team shall make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations. IT Team shall ensure proper security of cloud access tokens & implement appropriate security measures for testing, staging and backup environments hosted on cloud. IT Team shall disable/remove older or testing environments if their usage is no longer required.

Systems managed by vendors

Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) are managed by vendors and due to which we shall not be able to implement some of the aforementioned guidelines directly, we 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.

Periodic Audit

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

Version Management

Cyber Security Policy approved by BOD on 30th June 2023.

Version 1: Approved on 25th May, 2022 pursuant to SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022

Version 2: Approved on 30th June, 2022 pursuant to SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 & SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022.

Version 3: Approved on 20th March, 2023 pursuant to SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023