**Rameshwaram Capital Market**

## Policy on Cyber Security

Vide SEBI circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 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 brokers 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.

## SEBI Cyber Security Framework for Stock Brokers

The Uses of Information Technology in the securities market has grown rapidly and now it is an important part of the operational strategy for Stock Brokers. Recently the number of cyber incidents/attacks have increased in different way particularly securities and financial market . Market participator should urgently adopt the a robust cyber security/ resilience framework for protection the assets and resources adhering the SEBI/ Exchange provisions.

The guidelines annexed with this circular shall be effective from April 1, 2019.

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

1. Mr. Mahesh Kumar Gupta Proprietor
2. Mr. Ripul Agarwal Manager
3. Mr Pawan Sharma Dealer

Out of the above. Mr Ripul Agarwal shall also be held as Designated Officer for the purpose of this policy

Cyber Security Framework define and implement with reference to Circular SEBI/HO/MIRSD/CIR/PB/2018/147

**Protection:**

No un authorised person, irrespective of his/her designation, post or rank should have right to access critical systems, confidential data, applications or facilities. Password Policy is made mandatory for all level of data access with sufficient complexity of the Password placed. Any access given shall be for defined period and defined purpose only. QSL 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.

The access to the IT systems, applications, databases and networks needs to be sent on mail approved by immediate superior.

Two Factor Authentication 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 Five (5) 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 QSL after verification of the Customer's identity etc.

QSL 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.

QSL 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 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 unauthorised 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.

## Hardening of Hardware and Software

Procurement of all the hardware and software shall be done from reputed / experienced vendor/supplier only in company sealed packaging, 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 professional 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 / inhouse 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

IT professional 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.

IT professional 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.

## 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)

IT professional with the help of IT Experts shall time to time conduct vulnerability assessment to detect security vulnerabilities in the IT environments exposed to the internet.

Penetration test shall also be carried out once in a year

In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, IT professional shall report them to the vendors and the management 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 vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time

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

**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 shall be submitted to Stock Exchanges.

**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.

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

**Systems managed by vendors**

Where the systems (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.

# POLICY ON SQUARING OFF CLIENT POSITIONS IN CASE OF NON PAYMENT OF FUNDS AND MARGINS

RCM is having the right to sell client's securities, both unpaid securities as well as collaterals deposited towards margins including those held in Client DP, or close out client's open positions, without giving notice to the client where there is a delay/failure of the client meeting the pay in obligations and / or there is a failure of the client to bring additional margins including that of MTM on real-time basis at any point of time, to cover the increase in risk in the dynamic market conditions.

In case of unpaid obligations on T+3 basis, RCM may sell the unpaid/partially paid securities. In addition RCM may sell the collaterals deposited by the client towards margins and or paid securities purchased by the client in earlier settlements where the sale proceeds of unpaid securities are inadequate to cover the pay in obligations and where the unpaid securities appear to be comparatively illiquid and cannot be sold at reasonable rates to the extent required. RCM may follow LIFO method for liquidation of securities but it may not be binding on it to follow this method in all cases.

Any positions squared off for nonpayment of Margins will be flagged in the Contract Note.

## Margin shortfalls in F & O

Positions of the client may be closed out to the extent of margin shortfall on the T+1 basis. While computing the margin shortfall value of unapproved securities shall not be considered. RCM reserves the right to consider the collateral.

RCM has a system in place to inform the clients of their Margin Obligation, Cash Obligation, Margin Short fall, Margin Penalty etc. through SMS, email, Website etc. Where by client is aware of the Margin/Cash Obligation that is to be fulfilled. The clients are provided with secured ID and Password to view their Contract Notes, Margin, Paying Obligations and all other financial position through our Web site *https://www.vselindia.com*

All Futures And Options Positions nearing to expiry, ending up with physical delivery, where the client had not deposited the shares in case of short position or full amount of the delivery obligations two days before the expiry, the client has to be close such positions 2 days before the expiry, failing which RCM reserves the right to square off the positions at its discretion but not under obligation.

In case of exercise of in the money options, as the STT calculated is on the Strike

+Premium, due care should be taken by the clients, In such cases, where there can be negative financials, RCM reserves the right to square off, But not under obligation.

## Intraday Positions

RCM shall have the right to sell client's securities or close out client's open positions but it shall not be under any obligations to undertake this exercise compulsorily. RCM shall therefore not be under any obligation to compensate/or to provide reasons of any delay or omission on its part to sell client's securities or close open positions of the client. The ultimate responsibility risk and liability of the trades are binding on the client.

In dynamic Market conditions, there can be sudden rise or fall in the shares or Commodity Prices, which can make sudden difference in MTM and the Margins, might be increased on real time due to unforeseen heavy market fluctuations. Hence apart from the Margin calls made by us, Clients are under obligation and bound to Monitor their positions and make good for the Margins including that of MTM, on real time basis, failing which the client would be under default and the positions may be reduced or squared off. The word default is extensive based on the circumstances of the Risk involved in the trade executed and Market Conditions.

## Penalties levied by the Exchanges

Further Exchanges levy various penalties on the member brokers on auction resulting from short deliveries, non-adherence to client wise exposure limits, client wise shortfalls in F & O Margin and for other reasons which may be defined by the Exchanges from time to time. RCM is therefore authorized by the client to pass on any penalty imposed by the Exchange/SEBI and or any other regulatory authority to the client, which arises on account of the client.

## Review Policy

This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

The policy may be Monitored and reviewed by the **PROPRIETOR/Compliance Officer** and place the changes in policy before the Board at the meeting.

## Approval Authority

This policy is as approved by the Management in its meeting held on 26/04/2023