NAME OF THE STOCKBROKER

CYBER SECURITY AND CYBER RESILIENCE POLICY

POLICY CONTROL

Version:	1.0
Version Date:	_____ (Date of Passing Board Resolution)
Approved by:	Board of Directors
Department in Charge:	
Frequency of Review:	Yearly or as and when any update comes change in the Relevant Regulation comes or any change in the Company's internal control or Structure whichever is earlier.

TABLE OF CONTENTS:

CYBER SECURITY AND CYBER RESILIENCE POLICY

I. INTRODUCTION:

The Company has designed its Information security, Cyber security and Cyber Resilience Policy based on the regulatory guidelines prescribed by SEBI and encompassing by the National Critical Information Infrastructure Protection Centre (NCIIPC). This policy is also designed to meet the requirements of multiple stock exchanges like the NSE, BSE, MCX and NCDEX.

II. SCOPE:

This policy covers company's critical assets and associated legal entitles. It protects the interests of investors in securities and promotes the development of, and to regulate the securities market. Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience.

III. GOVERNANCE:

This policy document is approved by the Board of Directors / Partners / Proprietor / Senior Management. The policy document is reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

This policy shall be implemented through Standards, guidelines, policy, procedures, SOP, Risk Management & Cyber Security Management framework.

We shall follow below supporting policies and guidelines and shall adopt the best practices as per the international standards such as ISO 27001, ISO 22301 and COBIT 5 etc., or their subsequent revisions, if any, from time to time.

i. Acceptable Usage Policy
ii. Access Control Policy
iii. Asset Management Policy
iv. Communication Security Policy
v. Cryptography Policy
vi. E-Waste Policy
vii. Human resource Security
viii. Information Security Compliance Policy
ix. Information Security Incident Management Policy
x. Information Security Policy

xi. Information Systems Acquisition Development and Maintenance Policy
xii. Operations Security Policy
xiii. Physical and Environmental Policy
xiv. Supplier Relationship Management Policy
xv. Website Security Policy
xvi. Vulnerability Assessment and Penetration Testing Policy
xvii. Network Security Assessment Policy
xviii. Investor Grievance Policy
xix. BCP / DR Policy
xx. Backup Policy
xxi. Incident Response Policy
xxii. Password Security Policy
xxiii. Risk Management Policy
xxiv. Risk Assessment Policy

IV. ROLES AND RESPONSIBILITY:

1. Designated Officer:

The company nominates Mr. _____ 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.

He should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework. He should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of the company towards ensuring the goal of Cyber Security.

He should accordingly 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.

2. Identification:

The Designated Officer should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, company 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. IT Security Policy identifies the rules and procedures for all users accessing and using an organization's IT assets and resources.

3. Internal Technology Committee (ITC):

The Board of Directors / Partners / Senior Management shall constitute internal Technology Committee comprising with following members:

Sr.no	Name of Committee Members	Designation

This Technology Committee shall on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board of Directors / Partners / Senior Management. Such review shall include review of current IT and Cyber Security and Cyber Resilience capabilities and set goals for a target level. It shall establish plans to improve and strengthen Cyber Security and Cyber Resilience.

The Board of Directors / Partners / Senior Management should accordingly 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. 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.

V. PROTECTION:

1. Access Controls:

No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. We 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 should be for the period when the access is required and should be authorized using strong authentication mechanisms.

The company shall implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. All critical systems accessible over the internet would have two-factor security.

We shall ensure 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_____ (___) years. They should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to the company'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.

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 of the company, should be subject to stringent supervision, monitoring and access restrictions.

Internet access policy is in place 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 company's critical IT infrastructure. User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

2. **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.

We would 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.

3. **Data Security:**

Critical data must be identified and encrypted using strong encryption methods such as masking of critical information, masking of passwords while logging in, encrypted transfer of password to server etc. Measures are taken 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. Only authorized data storage devices within their IT infrastructure through appropriate validation processes. Use of mobile phones shall not be allowed to any employees for dealing with clients as well as any other external parties.

VI. NETWORK SECURITY POLICY:

The company establishes 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 should be secured within the Company's premises with proper access controls. All remote access the company will either be through a secure VPN connection on owned device of the company that has up-to-date anti-virus software, or on approved mobile devices.

Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the network without IT approval. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system or alter network hardware in any way. Every individual as well as network connected system shall have an Anti-Virus Software with Anti Malware and Anti Ransomware protection.

VII. HARDENING OF HARDWARE AND SOFTWARE:

Only hardened hardware / software is deployed, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system. 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. 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.

VIII. APPLICATION SECURITY IN CUSTOMER FACING APPLICATION:

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.

IX. CERTIFICATION OF THE OFF-THE SHELF PRODUCTS:

IT Team shall 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 4. 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.

X. PATCH MANAGEMENT:

IT Team shall 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. IT Professionals should 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 does not impact other systems.

XI. DISPOSAL OF DATA, SYSTEMS AND STORAGE DEVICES:

Suitable policy for disposal of storage media and systems is in place. 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.

XII. VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT):

IT Team 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 by the company, 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.

The company shall conduct VAPT at least once in a financial year from only CERT-In empaneled 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.

In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empaneled 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. In addition, the Company 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.

XIII. MONITORING AND DETECTION:

We shall establish 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, 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.

XIV. 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. IT officials shall ensure that we should 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 analysed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

XV. SHARING OF INFORMATION:

Quarterly reports containing information on cyber-attacks and threats experienced 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 should be submitted to Stock Exchanges / Depositories.

XVI. 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. Where possible, this should be extended to outsourced staff, vendors etc. The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

XVII. SYSTEMS MANAGED BY VENDORS:

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

XVIII. SYSTEMS MANAGED BY MIIs:

Where 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.

XIX. PERIODIC AUDIT:

We shall arrange to have our system audited on annual basis and shall obtain certification from any CERT-IN empaneled 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 / Partners / Proprietor of the company within three months of the end of the financial year.

XX. CLARIFICATION/INFORMATION:

In case of any clarification/information required on the implementation of the Policy, please contact the IT Head/Compliance Officer on Email -_____, Tel No._____.

XXI. REVIEW:

The said policy shall be reviewed by the Board of the Directors on a yearly basis or as and when any update comes change in the Relevant Regulation/Circular comes or any change in the (Name of the Stock Broker)'s internal control or Structure. The Compliance officer has the authority to give direction to undertake additions, changes, and modifications, etc. to this Policy, and the same shall be effective per the authority of the Compliance Officer and thereafter be ratified by the Board of the Directors at its next review.

X-X-X-X-X