COMPANY NAME – FOCUS STOCK BROKERS LTD

CYBER SECURITY AND CYBER RESILIENCE POLICY

Policy prepared by	Policy Reviewed by	Date of Review
Mr. RAMESH KUMAR	Mr. SIDDHANT MANTRY	23-Feb-2023

CYBER SECURITY AND CYBER RESILIENCE POLICY

1. STATUTORYMANDATE

This framework is formed by the requirements of the SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated, SEBI/HO/MIRSD/DOP/CIR/P/2019/109, and SEBI/HO/IMD/DOF2/P/CIR/2022/81.

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.
In Addition to the above Cyber security policy shall detect, prevent and mitigate Cyber-attack sand threats which attempt to compromise the Confidentiality, Integrity d Availability(CIA) of the computer systems, networks, and databases (Confidentiality refers to limiting access to systems and information to authorized users, assuring integrity hat the information's reliable and accurate, and Availability refers to guarantee of reliable access to the system and information authorized users). The 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 operations during, and recover from, a cyber-attack.

3. APPLICABILITY

Provisions of the said circular and framing of cyber security and cyber resilience are required to be complied with by all Stock Broker sand Depository Participants registered with SEBI.

The policy has been considered, take non record, and approved by the board of directors of the company at their duly convened meeting held on March 7, 2019.

4. SCOPE OF THE FRAMEWORK

Cyber-attack sand 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). The cyber security framework includes measures, tools, and processes that are intended to prevent cyber- attack sand improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operations during, and recover from, a cyber-attack.

With the view to strengthen and improve Cyber Security and Cyber Resilience framework, the board of directors of the company shall review these policy documents and their implementation there of at least once annually.

CYBER SECURITY AND CYBER RESILIENCE POLICY

5. DESIGNATED OFFICER

The company nominates Mr. Siddhant Mantry as the Designated Officer the company to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct these table and implementation of processes and procedures as per the Cyber Security Policy.

6. CONSTITUTION OF TECHNOLOGY COMMITTEE

6.1 The company constitutes a technology committee ("the committee") with the following members:

Sr.No.	Name of the Committee Members	Designation of the Members
1	Mr. Siddhant Mantry	Director
2	Mr. Anil Kumar Mantry	Director
3	Mrs Babita Mantry	Director
4	Ramesh Kumar	Compliance Officer

6.2 Such committee's hall on a half-yearly basis review the implementation of the Cyber Security and Cyber Resilience policy. Such review shall include but is not limited up to, reviewing current IT and Cyber Security and Cyber Resilience capabilities, setting up 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.

6.3 TheDesignated 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.

7. IDENTIFICATION, ASSESSMENT, AND MANAGEMENT OF CYBER SECURITY RISK

The company shall ensure the following steps in order to identify, assess, and manage Cyber Security risks associated with processes, information, networks, and systems.

7.1 IDENTIFICATION OF CRITICAL IT ASSETS AND RISKS ASSOCIATED WITH SUCH ASSETS

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 an 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.

7.2 PROTECTION OF ASSETS BY DEPLOYING SUITABL ECONTROLS, TOOLS, ANDMEASURES

In order to protect the cyber safety, the company shall ensure them erasures which include however not limited up to:

- Access controls
- Physical Security
- Network Security Management

- Data security
- Hardening of Hardware and Software
- Application Security in Customer-Facing Applications
- Certification of off-the-she lf 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 its assets of the company by deploying suitable controls, tools, and measures in conform it y with provisions of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 and any amendment or substitution thereof. However, the committee and designated officer of the company shall additionally deploy such measures in this respect, as maybe warranted from time to time.

7.3 DETECTION OF INCIDENTS, ANOMALIES, AND ATTACKS THROUGH APPROPRIATE MONITORING TOOLS/PROCESSES

Necessary steps as may be required to monitor and for early detection of unauthorized or malicious activities, unauthorized changes, unauthorized access, and unauthorized copying or trans mission of data/information held in a contractual or fiduciary capacity, by internal and external parties shall be maintained, appreciated and taken care on.

These crudity logs of systems, applications, and network devices exposed to the internet shall also be, from to time, monitor for anomalies, If any.

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

7.4 RESPONDING BACK BY TAKING IMMEDIATE STEPS AFTER IDENTIFICATION OF THE INCIDENT, ANOMALY, ORATTACK

The alerts are generated from monitoring and detection of systems in order to determine activities that are to be performed to prevent the expansion of such incident of cyber-attack or breach, mitigate its effect, and eradicate the incident.

In case of affection of systems by incidents of cyber-attacks or breaches, the company shall ensure timely restoration of the same in order to provide uninterrupted services. The committee and designated officer shall ensure to have the same Recovery Time Objective (RTO) and Recovery point objective (RPO) as per regulatory requirements.

With a view to providing quick responses to such cyber-attacks, the committee shall formula tea response plan defining responsibilities and actions to be perform edgy its employees and support/out sourced staff in the event of cyber-attacks or breaches of Cyber Security mechanisms. Such plan and any modification there in shall be circulated among stall the employees and support/outsourced staff from time to time.

7.5 RECOVERY FROM INCIDENT(S) THROUGH INCIDENT MANAGEMENT AND OTHER APPROPRIATE RECOVERY MECHANISMS

The company shall consider the outcomes of any incident of loss or destruction of data or systems and accordingly shall take precautionary measures to strengthen the security mechanism and improve recovery planning and processes.

Periodic check stoutest the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

8. The technology committee in accordance with the provisions of the said circular and formed here in after this frame work, shall ensure that this framework considers the principles prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) of the 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.

9. COMMUNICATIONOF UN USUAA CTIVITIES AND EVENTS

IT team of the company under the guidance of the committee shall monitor unusual activities and events and shall facilitate communication of the same to the 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 to the followings:

- To attend the cyber safety and training programs as conducted by the company from time to time.
- To endure installation, usage, and regular update of antivirus and antispyware software on the computers used by them.
- Use a fire wall 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 to limited employee access to data and information and limited authority to install the software.

- Regularly change passwords.
- Do not use or attach unauthorized devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on a 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.

Further, the company shall ensure that:

- No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources, or facilities.
- Any access to the systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. The company shall grant access to IT systems, applications, databases, and networks on a need-to-use basis and base don't he principle of least privilege. Such access shall be for the period when the access is required and should be authorized using strong authentication mechanisms.
- An access policy that addresses strong password controls for users' access to systems, applications, networks, and data bases shall be implemented.
- All critical systems accessible over the internet should have two-factor security (such as VPNs, Firewall controls, etc.), as far as possible.
- The company shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes, and such logs would be maintained and stored in a secure location for a time period not less than two(2)years.
- The Company shall be required to 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 shall inter-alia include restricting the number of privileged users, if any, period ic review of privileged users' activities, di sallow privileged users from accessing systems logs in which their activities are being captured, and strong controls over remote access by privileged users, etc.
- Employees and out sourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks, and other computer resources, shall be subject to stringent supervision, monitoring, and access restrictions.
- An Internet access policy to monitor and regulate the use of the internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within the company's critical IT infrastructure shall be formulated.
- User Management shall address the deactivation of access privileges of users who are leaving the organization nor whose access privileges have been withdrawn.
- Physical access to the critical systems shall be restricted to a minimum and only to authorized officials. Physical access of out sourced staff/visitors shall be properly supervised by ensuring at the minimum that out sourced staff/visitors are accompanied at all times by authorized employees.
- Physical access to the critical systems shall be revoked immediately if the same is no longer required.
- The company will ensure that the perimeter of the critical equipment room if any, shall be 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.

- The company shall establish 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 shall be secured within the premises with proper access controls.
- for algorithmic trading facilities, adequate measures shall be taken to I so late and secure the perimeter and connectivity to the servers running algorithmic trading applications, if any.
- The Company shall install network security devices, such as firewalls, proxy servers, and intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
- Adequate controls shall be deployed to address virus/malware/ransom are attacks. These controls May include host/network/application-based IDS systems, customized kernels for Linux, anti-virus and Anti-malware software, etc.
- Critical data shall be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexures A and B.
- the company shall implement measures to prevent authorized access or copying or trans mission of Data / information held in a contractual or fiduciary capacity. Its hall ensure that the confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- this security policy also covers the use of devices such as mobile phones, faxes, photocopiers, scanners, etc., with in their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, network connectivity for such devices, etc.
- The Company shall allow only authorized data storage devices with in their IT infrastructure through appropriate validation processes.
- The Company shall 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.
- Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data shall be blocked and measures are taken to secure them.
- 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. Required measures for ensuring security in such applications shall been sured.
- The company shall ensure that off-the-shelf products, if any, 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-houses of t ware and components need not obtain he certification but have to undergo intensive regression testing, configuration testing, etc. The scope of tests shall include business logic and security controls.
- The company establishes and ensures that the patch management procedures include the identification, categorization, and prioritization of patches and updates. An implementation time frame for each category of patches should be established to apply them promptly.

CYBER SECURITY AND CYBER RESILIENCE POLICY

- The Company shall perform rigorous testing of security patches and updates, where possible, before deployment in to the production environment so as to ensure that the application of patches does not impact other systems.
- Suitable policy for disposal of storage media and systems shall be frame dismay be required. The critical data/Information on such devices and systems shall be removed by using methods such as crypto shredding/degauss/Physical destruction as applicable.
- The Company shall formulate a data-disposal and data-retention policy to identify the value and life time of various parcels of data.
- The company shall regularly conduct a vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet, as and when required.
- The company with systems publicly available over the internet shall also carry out penetration tests, 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.
  In addition, the company shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.
- In case of vulnerabilities discovered in off-the-shelf products (used for core business)or applications provided by exchange empaneled vendors, the company shall report them to the vendors and the exchanges promptly.
- Remedial actions, if required, shall be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.
- The company 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 a 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 a anomalies if any.
- Further, to ensure higher silience, high availability, and timely detection of attacks on systems and networks exposed to the internet, the company shall implement suitable mechanism stom on it or the capacity utilization no fits critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
- Alerts, if any, generated from monitoring and detection systems shall be suitably investigated to deter mine activities that are to be performed to prevent the expansion of such incident of cyber-attack or breach, mitigate its effect, and eradicate the incident.
- the response and recovery plan of the company shall 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. The company shall have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements.
- Responsibilities and actions to be performed by the company's employees and support/outsourced staff in the event of cyber-attacks or b reach of the Cyber Security mechanism shall be defined.
- Any incident of loss or destruction of data or systems shall be thoroughly analyzed and lessons learned from such incidents shall be incorporated to strength he n the security mechanism and improve recovery planning and processes.
- Suitable periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

CYBER SECURITY AND CYBER RESILIENCE POLICY

11. SUBMISSIONOFQUARTERLYREPORTS

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.

12. TRAINING AND EDUCATION

The committee and designated officer shall conduct training and educational sessions for employees to make them aware of building Cyber Security and basic system hygiene awareness, to enhance knowledge of IT/Cyber Security Policy and standards among the employees by 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.

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), e.g. :NSE's NOW, BSE's BEST, etc., the responsibility of ensuring Cyber Resilience on those applications resides with the MIIs and not with the company. In such a case, the company is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

15. PERIODIC AUDIT & REVIEW

- The company shall arrange to have its systems audited on an annual basis by a 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/ Committee/any committee thereof within three months of the end of the financial year, Furthermore, the company shall also get certified from empaneled auditor for Vulnerability Assessment and Penetration Testing (VA-PT)as suggested by SEBI on yearly basis.

- The policy shall be reviewed on yearly basis and as and when required by the law for the time being the force

CYBER SECURITY AND CYBER RESILIENCE POLICY

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

CYBER SECURITY AND CYBER RESILIENCE POLICY

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 aadhaar number is play only a portion fit, enough for the Customer to identify, but use less to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if the aadhaar numbers "123456789", consider displaying something akin to "XXXXXX789" instead of the whole number. This also has the added be ne fit of not having to transmit the full piece of data over various networks.
3. Analyze data and data bases holistically and draw out meaning full "silos" (physical or virtual) in to 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 data bases. 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 being 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 have no public access end points, 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.

CYBER SECURITY AND CYBER RESILIENCE POLICY

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 servers mandatory, making the transport channel HTTP(S).
3. Avoid the use of In secure protocols such as FTP (File Transfer Protocol) that can be easily com promised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SS Hand VPN tunnels, RDP (with TLS), etc.

CYBER SECURITY AND CYBER RESILIENCE POLICY

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 pass phrases have more entropy and offer better security in general. Stock Brokers should attempt to educate Customers on these best practices.
2. Passwords, security PINs, etc. should never best or ed in plaintext and should be one-way has hed using strong crypto graphic has h functions (e.g.:bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password has he s are never transformed in to the original plaintext value sunder any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software crypto graphic tokens, VPNs, biometric devices, PKI, etc.). In the case of IBTs and SWSTs, a minimum of two factors in the authentication flow are mandatory.
4. In the case of Applications installed on mobile devices (such as smartphones and tablets), a crypto graphically secure biometric two-factor authentication mechanism may be used.
5. After are as on able number off ailed log in attempts in to 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 crypto graphic all y 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 pass phrases. 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.