Obsidian Investment Private Limited
CYBER SECURITY AND CYBER RESILIENCE POLICY

601/605, HET DIV SQUARE, BEHIND HOTEL MARRIOT,SINDHU BHAVAN ROAD,BODAKDEV AHMEDABAD380054
Contact : +91 9737222149 E-mail : admin@obsidiancapital.in
CIN: U64990GJ2025PTC162598

1. STATUTORY MANDATE

SEBI has issued circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019, SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022, SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 and SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023 providing guidelines on Cyber Security and Cyber Resilience. The objective of the said circular is to adapt to the rapid technological developments in Securities Market which have highlighted the need for robust Cyber and Cyber Resilience at the level of Stock brokers/Depository participants who are performing significant functions in providing services to the holder of Securities.

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.

3. APPLICABILITY

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

The policy has been considered, taken on record and approved by the board of directors of the company at their duly convened meeting held on 25th July 2026.

4. SCOPE OF THE FRAMEWORK

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems , net works 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). 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 operation 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 this policy documents and implementation thereof at least once annually.

5. DESIGNATED OFFICER

The company nominates Mr. Mukul Agrawal 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.

6. CONSTITUTION OF TECHNOLOGY COMMITTEE

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

Sr. No	Name of the Committee Members	Designation of the Members
1	Mr. Karna Agrawal	CISO & Designated Director
2	Mr. Aditya Ramachandran	COO

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

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 risk 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 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 SUITABLE CONTROLS, TOOLS AND MEASURES

In order to protect the cyber safety, the company shall ensure the measures which include, however not limited upto:

- Access controls
- Physical Security
- Network Security Management
- Data security
- Hardening of Hardware and Software
- Application Security in Customer Facing Applications
- Certification of off the shelf 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 assets of the company by deploying suitable controls, tools and measures in conformity with the provisions of SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018 and any amendment or substitution thereof. However, the committee and designated officer of the company shall additionally deploy such measures in this respect, as may be 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 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 shall be maintained, appreciated and taken care on.

The security logs of systems, applications and network devices exposed to the internet shall also be, from to time, monitored 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 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 OR ATTACK

The alerts generated from monitoring and detection of 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.
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 formulate a response plan defining responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber attacks or breach of Cyber Security mechanism. Such plan and any modification therein shall be circulated amongst all 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 take into account 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 checks to test 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 hereinafter this framework, shall ensure that this framework considers the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of 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. COMMUNICATION OF UNUSUAL ACTIVITIES AND EVENTS

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

- To attend the cyber safety and trainings programs as conducted by the company from time to time.
- To endure installation, usage and regular update of antivirus and antispyware software on computer used by them.
- Use a firewall 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 WiFi network secured and hidden.
- To adhere limited employee access to data and information and limited authority to install software.
- Regularly change passwords.
- Do not use or attach unauthorised devices.
- Do not try to open restricted domains.
- Avoid saving your personal information on computer or any financial data on any unauthentic website.
- To get your computer regularly scanned with antivirus software.
- Do not release sensitive data of the organization.

11. SUBMISSION OF QUARTERLY REPORTS

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 on building Cyber Security and basic system hygiene awareness, to enhance knowledge of IT / Cyber Security Policy and standards among the employees 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), 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. In such case, the company is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

15. PERIODIC AUDIT

The company shall arrange to have its systems audited on an annual basis by a CERT- IN empanelled 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.