

POLICY ON CYBER SECURITY & CYBER RESILIENCE FRAMEWORK

➤ **PURPOSE**

The purpose of this Policy is to maintain robust cyber security and cyber resilience framework to protect the integrity of data and guard against breaches of privacy, provide essential facilities to our clients and perform systemically critical functions relating to securities market.

➤ **MEANING**

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.

➤ **MONITORING**

This Policy include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:

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

➤ **APPOINTMENT OF DESIGNATED OFFICER**

Mr. Siddharth Kothari (Desgn. System Administrator) has been appointed as our designated officer.

➤ **ROLE OF DESIGNATED OFFICER**

The role of the designated officer is to perform the following duties:

- access, identify, and reduce security and Cyber Security risks
- respond to unwanted incidents
- Establish appropriate standards and controls
- direct the establishment and implementation of processes and procedures as per the Cyber Security Policy
- periodically review instances of cyber-attacks

- take appropriate steps to strengthen Cyber Security and cyber resilience framework.
- Maintenance of up-to-date inventory of 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.

➤ **CONSTITUTION OF INTERNAL TECHNOLOGY COMMITTEE**

The Board of directors of MLB Stock Broking Pvt. Ltd. has formed an internal technology committee comprising of IT in-house experts. The function of the committee is to:

- Review the implementation of the Cyber Security and Cyber Resilience policy on half-yearly basis
- Review of current IT and Cyber Security and Cyber Resilience capabilities
- Set goals for a target level of Cyber Resilience
- Establish plans to improve and strengthen Cyber Security and Cyber Resilience
- Periodically review instances of cyber-attacks
- Take appropriate steps to strengthen Cyber Security and cyber resilience framework.

➤ **Policy on Access Controls**

- No person should have any intrinsic right to access confidential data, applications, system resources or facilities of the company.
- Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period.
- Any access to IT systems, applications, databases and networks should be 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
- Strong password controls should be implemented for users' access to systems, applications, networks and databases.
- All critical systems of the company accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)
- Records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes.
- User access logs of every user should be maintained and stored in a secure location for a time period not less than two (2) years.
- Deploy necessary controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to the critical systems of the company by 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.
- Supervise, monitor and restrict the authorized access may be given to own employees and outsourced staffs of vendors or service providers.

- Address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

➤ **Policy on Physical Security**

- Physical access to the critical systems of the company should be restricted to minimum and only to authorized officials.
- Physical access of outsourced staff/visitors should be properly supervised and should be accompanied at all times by authorized employees.
- Physical access to the critical systems should be revoked immediately if the same is no longer required.
- The critical equipment rooms are physically secured and monitored by authorized employees with the help of CCTVs and Biometric access systems.

➤ **Network Security Management**

- Network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to should be installed to protect IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.
- Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.

➤ **Data Security**

- Critical data shall be identified and encrypted in motion and at rest by using strong encryption methods
- Unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity shall be strictly restricted.
- Do not compromise with the confidentiality of information during the process of exchanging and transferring information with external parties.
- Capturing and transmission of sensitive data using devices such as mobile phones, faxes, photocopiers, scanners, etc. are not allowed without permission. Only authorized data storage devices are allowed through appropriate validation processes.

➤ **Hardening of Hardware and Software**

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.

Any open port on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and appropriately handled to secure them.

➤ **Application Authentication Security**

- All Applications like IBT trading application, Back office application etc. offered to clients should be password protected.
- Educate clients with the usage and security of the applications offered to them.
- In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
- In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
- The account of the clients shall be locked in case of failed login attempts and login shall be allowed after complete authentication of user of the application.

➤ **Patch Management**

- Patch management procedure should include the identification, categorization and prioritization of patches and updates.
- Rigorous testing of security patches and updates, where possible, shall be performed before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

➤ **Disposal of data, systems and storage devices**

Disposal of storage media and systems shall be done in a proper manner as per the Data Retention and Data Disposal policy.

➤ **Vulnerability Assessment and Penetration Testing (VAPT)**

- Assessment of vulnerability should be done on regular basis to detect security vulnerabilities.
- Systems publicly available over the internet should 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.
- Perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

- Report about the vulnerabilities discovered in off-the-shelf products or applications 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**

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,
- 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 should also be monitored for anomalies.

Implement suitable mechanisms to monitor capacity utilization of the critical systems and networks that are exposed to the internet such as firewalls to monitor bandwidth usage and others.

➤ **Response and Recovery**

Alerts generated from monitoring and detection systems shall 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.

Timely restore systems affected by incidents of cyber-attacks or breaches.

The response plan should define 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.

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.

Conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.

➤ **Strengthening the Regulatory framework**

- To develop a dynamic legal framework and its periodic review to address the cyber security challenges
- To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.
- To enable, educate and facilitate awareness of the regulatory framework among employees.

➤ **Training and Education**

- Create awareness about Cyber Security among technical and non-technical staffs.
- 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. This training program may be extended to outsourced staff, vendors etc.
- The training programs should be reviewed and updated regularly.