Cyber Security Policy

Statutory mandate: This framework is formed in accordance with the requirements of the SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated December 3, 2018.

Preface:Rapid technological advancements in the securities industry have brought to light the importance of having a strong cyber security and cyber resilience framework to preserve the int egrity of data and prevent privacy breaches.
It is desirable for ASTHATRADE to have a strong cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to the securities market, as the stock broker and depository participant perform significant functions in providing services to holders of securities.

Based on their sensitivity and criticality for corporate operations, services, and data management, ASTHATRADE shall identify and classify critical assets. Business-critical systems, internet-facing apps and systems, systems containing sensitive data, including sensitive financial data, sensitive personal data, and Personally Identifiable Information (PII) data, are examples of critical assets. All support systems that are utilized to connect to or communicate with critical systems for either operations or maintenance must also be categorized as critical systems. The list of important systems must be approved by the ASTHATRADE's Board.

To this end, ASTHATRADE shall maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows

Need of Policy:

Every stock broking entity as well as depository participant is required to Identify, assess and manage the Cyber Risks associated with processes, information, networks and systems. In ASTHATRADE, in order to achieve the above target, a need of policy for cyber security arose.

Cyber Security Framework and Policy:

ASTHATRADE shall follow below 5 Point framework for Cyber Security and Cyber Resilience Framework:

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

To implement the above framework, an Internal Technology Committee shall be formed comprising of following individuals:

1. Mr. Satish Chandra Gupta — Director
2. Mr. Shauryam Gupta — Chief Technology Officer
3. Mr. Gyanesh Srivastava — Information Technology Manager

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

Mr. Satish Chandra Gupta shall be held liable for this policy, in absence of Chief Technological Officer and Information Technology Manager and all the roles assigned to CTO and IT Manager shall be accordingly reassigned to Mr Satish Chandra Gupta.

Identification: Mr. Gyanesh Srivastava, Information Technology Manager of the company will identify all the critical assets based on their sensitivity and criticality for business operations and shall maintain an Up to Date Inventory of its hardware and systems along with name and ID details of personnel to whom such hardware and systems are issued. He shall also be held responsible to identify the software installed, details of network, data flowchart and connection to the networks.

Mr. Gyanesh Srivastava along with guidance of Mr. Shauryam Gupta and external agencies (if required), shall identify the cyber risks that ASTHATRADE may face along with the likelihood and impact of the same on business of company.

Protection:

No unauthorized person, irrespective of his/her designation, post or rank should have right to access critical systems, confidential data, applications or facilities.

Any access given shall be for defined period and defined purpose only. ASTHATRADE 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.

Any Application offered by ASTHATRADE 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 minimum length of 6 characters of complex password shall be enforced across the applications. An attempt to educate the customers shall also be made by team.

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 Three (3) 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 ASTHATRADE after verification of the Customer's identity etc.

ASTHATRADE 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.

ASTHATRADE 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, card access systems, mantraps, bollards, 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 unauthorized 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 authorised 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 and any call to clients shall be made using baseline phones having voice logger facility only.

Hardening of Hardware and Software

Procurement of all the hardware and software shall be done from renowned vendor/supplier only in company sealed packaging and any unauthorized software and hardware shall not be installed on any system, 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 team 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 / 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.

Patch management

Team 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.

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

ASTHATRADE 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 as ASTHATRADE 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.

ASTHATRADE shall conduct VAPT at least once in a financial year. ASTHATRADE required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity. In addition, Stock Brokers / Depository Participants 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.

Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges / Depositories within 3 months post the submission of final VAPT report.

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

Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depositories Participants shall be reported to Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting such incidents or being brought to notice about such incidents. The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-
In from time to time. Additionally, the Stock Brokers / Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Stock Brokers / Depository Participants 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 / Exchanges /Depositories and SEBI shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year. The above information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.

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 (IBT, 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.

Last reviewed on :19.05.2023