ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

CYBER SECURITY AND CYBER RESILIENCE POLICY

Version	2024/01/02	Original Adoption Date:	01/04/2019
Review Date	05/04/2024		
Review & Approved by		Reviewed by Technology Committee & Approved by Board of Directors	

Background and Objectives

This Policy highlights emerging supervision practices that contribute to to effective cybersecurity risk supervision, with an emphasis on how these practices can be adopted by Stock Broker and DP (herein after referred as "Member")that are at an early stage of developing a supervisory approach to strengthen cyber resilience. Stock Brokers/DPs are working to establish and implement a framework for cyber risk supervision.

Cyber risk often stems from malicious intent, and a successful cyber attack—unlike most other sources of risk—can shut down a financial intermediary immediately and lead to system wide disruptions and failures. The probability of attack has increased as financial systems have become more reliant on information and communication technologies and as threats have continued to evolve.

Own risk management is the first line of defence in case of financial intermediaries but supervisory controls plays important role in ensuring resilience of intermediary and systems. The financial sector is a high-profile target for cyber threat actors, and cyber risks are a danger to the stability of national and global financial systems owing to potential cross-border spillovers. The financial sector is highly, and increasingly, dependent on information and communication technologies (ICT). A cyber attack can disrupt the provision of critical functions, threaten liquidity, and destabilize the integrity of the financial system. Strengthening cybersecurity in the financial sector is a priority for financial stability.

About Policy Framework

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. 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 clients having trading and demat account with member.

It is desirable that member have robust cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.
As per SEBI Circular, Stock Broker and DPs are required to identify, assess and manage the cyber risk associated with processes, information, network and systems and create policy framework covering following aspects;

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

As per above referred SEBI Circular, Member need to constitute "Technology Committee" and also appoint designated officer for the purpose of this policy.

The same is as per Annexure A to this policy.

APPLICABILITY & SCOPE

This Policy is applicable to member with effect from 01st April, 2019. The policy has been considered, taken on record and approved by board of directors of the company and further, technology committee has been set up and designated office has been appointed as per Annexure A to this circular.

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.

The designated officer is required to 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.

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases.

- Whereas, 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 at least once annully and implementation thereof at least half yearly. 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.

IDENTIFICATION OF CRITICAL IT ASSETS AND RISKS ASSOCIATED

A key component of the risk management program is the identification of critical assets, information and systems, including order routing systems, risk management systems, execution systems, data dissemination systems, and surveillance systems. Practices supporting the identification function include the establishment and maintenance of an inventory of all hardware and software. This risk management program should also typically include third-party and technology providers' security assessments. Finally, accessing information about the evolving threat landscape is important in identifying the changing nature of cyber risk.

Member can receive threat reports from external vendors on data traffic and fraudulent sites, access vendor feeds, security bulletin service providers, information from CERT-In and other information sharing platforms.

Designated officer in consultation with technology committee shall identify critical assets based on their sensitivity, criticality for business operations and exposure to outside network and maintain uptodate list of inventory consisting of hardware and software along with details of personnel to whom such hardware and/or software issued. Designated officer shall also be responsible to identify the software installed; Network details, data flow chart and connection to networks (Network Diagram).

PROTECTION OF CRITICAL IT ASSETS

The "Protection" core function aims at developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of its assets and services. These measures should be proportionate to and consistent with Member's risk tolerance, threat landscape and systemic role in the financial system. Member should implement appropriate and effective measures in line with leading cyber resilience and information security practices to prevent, limit or contain the impact of a potential cyber event.

Controls: Member has to implement appropriate protective controls that are in line with leadingpractice cyber resilience standards to minimise the likelihood and impact of a successful cyber attack on identified critical business functions, information assets and data.

Protective controls should be proportionate to and consistent with the Member's risk tolerance, its threat landscape and its systemic role in the financial system.

Resilience by design: Member has to consider cyber resilience from the ground up during system and process design, as well as service and product development, in order to minimise the probability of a successful cyber attack. A process to instil resilience by design should ensure that all software, network configurations and hardware, for example, are subject to rigorous testing against related security standards, that attack surfaces are limited to the extent practicable, and that common information security principles are adhered to, such as ensuring that access to systems is restricted to those with a legitimate business requirement.

Strong ICT controls: Member has to consistently maintain a strong ICT control environment, this being a fundamental and critical component of an FMI's overall cyber resilience. Such strong controls include;

a. Implementing appropriate measures to protect information (both in transit and at rest), commensurate with the criticality and sensitivity of the information held by and transmitted through Member. This should include, but not be restricted to, appropriate encryption (eg end to-end encryption) and authentication measures (eg multifactor authentication).
b. Ensuring that the Member has a comprehensive change management process that explicitly considers cyber risks, in terms both of residual cyber risks identified prior to and during change and of any new cyber risk created post-change.
c. Ensuring that a process exists to identify patches to technology and software assets, evaluate the patch criticality and risk, and test and apply the patch within an appropriate time frame.
d. Configuring ICT systems and devices with security settings that are consistent with the expected level of protection.

Member need to establish baseline system security configuration standards to facilitate consistent application of security settings to operating systems, databases, network devices and enterprise mobile devices within the ICT environment. Regular enforcement checks should also be performed to ensure that non-compliance with such standards is promptly rectified.

Layered protection that facilitates response and recovery: Member has to enable protective controls for the monitoring and detection of anomalous activity across multiple layers of the infrastructure, which requires a baseline profile of system activity. Controls should be implemented in a way that will assist in monitoring for, detecting, containing and analysing anomalous activities should protective measures fail. For example, (re-)designing processes to introduce more segmentation, intermediate checkpoints and intermediate reconciliations may allow quicker detection, identification and repair/recovery from a disruption.

Similarly, segmenting networks in a manner that segregates systems and data of varying criticality may have multiple benefits, both by helping the member to insulate systems in one segment from a security compromise in other segments, and by facilitating more efficient recovery of services. The latter benefit is achieved because, in the event of such a compromise, only the affected segments have to be restored, rather than the entire ICT infrastructure and all data sets.

Risks from interconnections: Member needs to implement protective measures to mitigate the risks arising from the entities within its ecosystem. The appropriate controls for each entity will depend on the risk that arises from the connected entity and the nature of the relationship with the entity. In view of its systemic importance and unique position in the financial system, member has to implement measures to mitigate effectively the risk arising from its connected entities, including the following:

a. Member's participation requirements should be designed to ensure that they adequately support its cyber resilience framework.
b. Member's framework to manage its relationship with service providers should address and be designed to mitigate cyber risks. At a minimum, member has to ensure that its service providers meet the same high level of cyber resilience they would need to meet if their services were provided by member itself. Cyber considerations should be integral part of member's arrangements for managing vendors and vendor products in the areas of contracts, performance, relationships and risk. Contractual agreements between member and its service providers should ensure that Member and relevant authorities are provided with or have full access to the information necessary to assess the cyber risk arising from the service provider.

Insider threats:

Security analytics: Member is required to, within the relevant legal framework, implement measures to capture and analyse anomalous behaviour by persons with access to its systems. Data loss identification and prevention techniques need to be employed to protect against the removal of confidential data from the member's network.

Changes in employment status: Member is required to conduct screening/background checks on new employees to mitigate insider threats. Similar checks should be conducted on all staff at regular intervals throughout their employment, commensurate with staff's access to critical systems. Member is also required to establish processes and controls to mitigate risks related to employees terminating employment or changing responsibilities.

Access control: Physical and logical access to systems should be permitted only for individuals who are authorised, and authorisation should be limited to individuals who are appropriately trained and monitored. Member is required to ensure that such access to systems is restricted only to those with a legitimate business requirement. In particular, Member is required to institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication, and monitoring for anomalies should be implemented.

To conclude, Member is required to implement following measusres to protect its company from cyber attack.

- ➤ Access Controls (Role Based Access)
- ➤ Physical Security (Access Card/Register)
- ➤ Network Security Management
- ➤ Data Security
- ➤ Hardening of Hardware and software
- ➤ Application Security
- ➤ Certification of Off-the-shelf products
- ➤ Patch Management
- ➤ Dispoal of data, systems and storage devices
- ➤ Vulnerability Assessment and Penetration Testing (VAPT)

ILLUSTRATIVE MEASURES FOR DATA SECURITY ON CUSTOMER FACING APPLICATIONS

1. Analyse 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 phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into 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 databases. 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 be in 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 has no public access endpoints, 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.

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 server is mandatory, making the transport channel HTTP(S).
3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

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 passphrases have more entropy and offer better security in general. Stock Brokers should attempt to educate Customers of these best practices.
2. Passwords, security PINs etc. should never be stored in plain text and should be one way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of 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 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 passphrases. 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 email and phone number) are up-to-date.
7. Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

DETECTION OF INCIDENTS, ANOMALIES AND ATTACKS

In order to have strong Cyber Resilience, member must have system to recognise signs of a potential cyber incident, or detect that an actual breach has taken place.

Early detection provides Member with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the

impact of the attack – for example, by preventing an intruder from gaining access to confidential data or exfiltration of such data. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, Member should maintain effective capabilities to extensively monitor for anomalous activities.

Continuous monitoring: Member should establish capabilities to continuously monitor (in real time or near real time) and detect anomalous activities and events. These capabilities should be adaptively maintained and tested.

Comprehensive scope of monitoring: Member should monitor relevant internal and external factors, including business line and administrative functions and transactions. Member should seek to detect both publicly known vulnerabilities and vulnerabilities that are not yet publicly known, such as so-called zero-day exploits, through a combination of signature monitoring for known vulnerabilities and behaviourally based detection mechanisms. Detection capabilities should also address misuse of access by service providers or other trusted agents, potential insider threats and other
advanced threat activity. These processes should be informed by and integrated with a strong cyber threat intelligence programme.

Layered detection: The ability to detect an intrusion early is critical for swift containment and recovery. Member should take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes and technology, with each layer serving as a safety net for preceding layers. In addition, an effective intrusion detection capability could assist Member in identifying deficiencies in their protective measures for early remediation.
Incident response: Member's monitoring and detection capabilities should facilitate its incident response process and support information collection for the forensic investigation process.

Security analytics: Member should implement, within relevant legal boundaries, measures to capture and analyse anomalous behaviour by persons with access to the corporate network.

RESPONSE TO INCIDENTS, ANOMALIES AND ATTACKS

Financial stability may depend on Members' ability to settle obligations when they are due. Therefore, Member's arrangements should be designed to enable it to resume critical systems rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them. Continuity planning is essential in meeting related objectives.

Upon detection of a successful cyber attack or an attack attempt, Member should perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is ongoing, FMIs should also take immediate actions to contain the situation to prevent further damage and commence recovery efforts to restore operations based on their response planning.

Member should be able to resume critical operations rapidly. An FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios.

While Member should plan to safely resume critical operations within two hours of a disruption, they should also plan for scenarios in which this objective is not achieved. Member should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, depending on the design of Member, facilitate the processing of critical transactions, for example, while remediation efforts continue. Member should also plan for situations where critical people, processes or systems may be unavailable for significant periods – for example, by potentially reverting, where feasible and practicable, to manual processing if automated systems are unavailable.

Member should develop and test response, resumption and recovery plans. These plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of its assets, and to meet its settlement obligations. Plans should be actively updated based on current cyber threat intelligence, information-sharing and lessons learned from previous events, as well as analysis of operationally and technically plausible scenarios that have not yet occurred. Member should consult and coordinate with relevant internal and external stakeholders during the establishment of its response, resumption and recovery plans.

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.

RECOVERY FROM INCIDENTS

Member should design systems and processes to limit the impact of any cyber incident, resume operations within two hours of a disruption, complete settlement by day-end and preserve transaction integrity. The possibility to resume operations in a system that is technically different from the primary system may be one of the options taken into account. Member's incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity and disaster recovery planning and recovery operations, and coordinated with relevant internal and external stakeholders.

Contingency plan should ensure that the status of all transactions and member and clients' positions at the time of a disruption can be identified with certainty in a timely manner, Member should design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, Member's systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code), to be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls. In addition, cyber resilience framework should include data recovery measures, such as keeping a copy of all received and processed data (including the original intent of instructions), and maintaining transaction replay capability.

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.

COMMUNICATION OF UNUSUAL ACTIVITIES AND EVENTS

Member should plan in advance for communications with participants, authorities and others (such as service providers and, where relevant, the media). Communication plans should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Because rapid escalation of cyber incidents may be necessary, Member should determine decision-making responsibilities for incident response in advance, and implement clearly defined escalation and decision-making procedures. Member should inform relevant oversight and regulatory authorities promptly of potentially material or systemic 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. Within 06 hours any instance of Cyber-attacks, threats, cyber-incidents and breaches experienced shall be reported to SEBI on sbdp-cyberincidents@sebi.gov.in. and Cert-in on CERT-in incident@cert-in.org.in .

Further Member is required to appoint CISO - Chief Information Security Officers and intimate details to Cert-in on info@cert-in.org.in .

RESPONSIBILITIES OF EMPLOYEES, MEMBERS AND PARTICIPANTS

Member should have a policy and procedure to enable the responsible disclosure of potential vulnerabilities following a risk-based approach. In particular, Member should prioritise disclosures that could facilitate early response and risk mitigation by stakeholders for the benefit of the ecosystem and broader financial stability,

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 Wi-Fi 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 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 based on the 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 which addresses strong password controls for users' access to systems, applications, networks and databases 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 company's critical systems. Such controls and measures shall inter-alia include restricting the number of privileged users, if any, 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, shall be subject to stringent supervision, monitoring and access restrictions.
- 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 company's critical IT infrastructure shall be formulated.
- User Management shall address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
- Physical access to the critical systems shall be restricted to minimum and only to authorized officials. Physical access of outsourced staff / visitors shall 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 shall be revoked immediately if the same is no longer required.
- The company will ensure that the perimeter of the critical equipments 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 isolate 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, 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 / ransomware 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.
- The company shall implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It shall ensure that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- This security policy also covers use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
- The company shall allow only authorized data storage devices within 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 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 be ensured.
- 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-house software and components need not obtain the 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 timeframe for each category of patches should be established to apply them in a timely manner.
- The company 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.
- Suitable policy for disposal of storage media and systems shall be framed as may 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 lifetime of various parcels of data.
- The company shall regularly conduct 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 empanelled vendors, the company shall report them to the vendors and the exchanges in a timely manner.
- 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 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, if any.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, the company 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.

- ➤ Alerts, if any, 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.
- ➤ 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 company's employees and support / outsourced staff in the event of cyber-attacks or breach of 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 strengthen 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.

QUARTERLY SUBMISSION TO REGULATOR

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.

TRAINING, LEARNING AND EVOLVING

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.

To identify and distil key lessons from cyber events that have occurred within and outside the organisation in order to advance resilience capabilities. Useful learning points be gleaned from successful cyber intrusions and near misses in terms of the methods used and vulnerabilities exploited by cyber attackers.

To work towards achieving predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity. To consider acquiring New advanced technology to mitigate new form of cyber attacks and know-how to maintain its cyber resilience.

THIRD PARTY MANAGED SYSTEMS

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.

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.

The annual basis and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board / committee / any committee thereof within prescribed time line. Company shall arrange to have its systems audited on an half yearly/annual basis.

Disclaimer & Review

This policy & Procedure must be reviewed as and when there are regulatory amendments and in absence of any amendment, on yearly basis. The information contained in this material is intended only for the use of the entity to whom it is addressed and others authorized to receive it. It may contain confidential or legally privileged information. The addressee is hereby notified that any disclosure, copy, or distribution of this material or the contents thereof may be unlawful and is strictly prohibited.