CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK

SKP SECURITIES LIMITED

Sl No	Table of Content	Page
1	Objective	4
2	Scope	4
3	Applicability	4
4	Definitions	4-5
5	General	6
6	Risk Management Framework Identification and Classification of Assets Risk Identification and Assessment Process Identification Risk Treatment Risk Mitigation Reporting Risk Events Reporting Information Security Events Management of Information Security Incidents	7 -10
7	Cyber Security Preparedness Indicators Network Segmentation Implementation Secure Remote Access Usage Role Based Access Control Password Security Vulnerability Awareness and Patch Implementation Implement an Employee Cyber Security Training Program Involve Executives in Cyber Security Development of a Cyber Security Detection and Incident Response Plan	10- 11
8	Cyber Crisis Management Plan Types of Cyber Crisis Points for Action	11-14
9	Reporting of Information on Cyber Security Cyber Security Incident Recording and Incident Handling Cyber Incident Logging	14-15
10	Vulnerability and Patch Management Technical Vulnerability Management	15-16

	VAPT prior to the commissioning of a new system VAPT after any significant change Patching Reporting Security Weaknesses VAPT Result Records	
11	Cyber Security Awareness IS Awareness Agenda IS Awareness Program Management Security Incidents & Reporting	**17**
12	Access Management	**17-18**
13	Physical Security	**18**
14	Network Security Management	**18-19**
15	Data Security	**19**
16	Application Security	**20**
17	Disposal of data, systems and storage devices	**20**
18	Monitoring and Detection	**20-21**
19	BCP and DR	**21**
20	Compliance	**22-24**
21	Review	**24**
22	Exception	**24**
23	Annexure A	**25**
24	Annexure B	**26**
25	Annexure C	**26-27**

A. Objective

The objective of this document is to establish a Cyber Security & Cyber Resilience framework, in order to provide guidance on cyber security matters relating to technology, customers, suppliers, employees and other parties associated with SKP Securities Limited in compliance with applicable statutory requirements.

It is expected of all employees who are engaging with or whether on behalf of SKP Securities Limited or, in their personal capacity, to understand and to follow the below framework. This framework shall continue to evolve as new technologies emerge.

B. Scope

This document associated with of SKP Securities Limited, (hereafter referred to as "Company") elicits the practices of Cyber Security & Cyber Resilience framework that must be followed to ensure that the Company complies with the applicable statutory and/or regulatory requirements.

C. Applicability

This framework applies to individuals worldwide working for all affiliates and subsidiaries of the Company & its employees (whether permanent, fixed-term or temporary), consultants, contractors, third party staff, interns, trainees, agents associated with us are collectively referred to as "Users" in this policy). The framework shall operate in conjunction with other business and operating/administrative policies of the Company.

D. Definitions

1. **Company:** It refers to SKP Securities Limited herein referred to as "SKP".

2. **Users/You/Your :** It refers to every person who works at the Company, that is, employees (whether permanent, fixed-term or temporary), contractors, consultants, trainees, third-party staff, casual workers, volunteers, interns, agents including the senior management

3. **Cyber Crisis Management Plan (CCMP):** It is a part of the overall Board approved strategy that is developed in compliance with the Company's Cyber Security and Cyber Resilience Policy which addresses four aspects, i.e., Detection, Response, Recovery, and Containment.

4. **Cyber Security Preparedness Indicators**: It is a part of the Company's overall Risk Management framework to ensure that the adequacy of an adherence to the Company's Cyber Security and Cyber Resilience framework is accessed and measured through the development of indicators to assess the level of risk and/or preparedness.

5. **Confidentiality:** It refers to limiting access to systems and information to authorized users.

6. **Integrity:** It is the assurance that the information is reliable and accurate.

7. **Availability**: It refers to the guarantee of reliable access to the systems and information by authorized users.

8. **Cyber Security Framework:** It is a combination of measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience.

9. **Cyber Resilience:** It is the Company's ability to prepare and respond to a cyber-attack, continue operations during an attack, and recover from it.

10. **Social Media Risks**: It refers to the risks arising out of Social Media such as getting tricked by an Imposter Account, breach of privacy, etc

11. **Vulnerability:** It is the quality or state of being exposed to the possibility of being attacked or harmed.

12. **Vulnerability Assessment:** It is a process of identifying, quantifying, and prioritizing the vulnerabilities in a system.

E. General

This Cyber Security and Resilience Framework establish a framework to combat cyber threats of technology and information assets, given the level of complexity of business and acceptable level of risk. Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases .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.

The SKP encompasses the "Guidelines for the Protection of National Critical Information Infrastructure" of National Technical Research Organization (NTRO), updated from time to time, as per statutory requirements. This framework also encompasses best practices from international standards like ISO 27001 or their Subsequent revisions, if any, from time to time.

The SKP shall establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner. The Designated officer and the internal technology committee of the Company shall periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and Cyber Resilience framework.

The SKP shall have well-defined roles and responsibilities for its employees, outsourced staff, and employees of vendors, members or participants of other entities, who may have privileged access or use systems including the Company's network to ensure the goal of Cyber Security.

Mr Joy Saha , referred to as the "Designated Officer" as per SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 is responsible for assessing, identifying, reducing Cyber Security risks, responding to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per this Cyber Security and Cyber Resilience Policy. The Members of the Committee are : Mr Joy Saha (Designated Officer) , Mr Abhay (Sub

F. Risk Management Framework

SKP has defined a Risk Management Framework to (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.

1. Identification and Classification of Assets

An Asset is anything that has value to the Company. Laptop, desktop, printer, computer peripherals, storage, network devices, mobile devices, etc. are physical IT assets while assets such as software, online accounts, public certificates, etc. are termed as digital IT assets. The Company has classified the assets in the following categories:-

a. **Physical Assets:** - Assets that include the physical component(s) of the computer and computer networks are termed physical assets.

b. **Software Assets**: Assets include all software used by the SKP.

c. **Informational Assets:** All the assets that include documents produced or received, within the scope of the SKP operations, that is, paper or electronic in computer applications and systems for data processing and/or electronically processed data, required for the SKP smooth operations.

d. **Service Assets** Resources are termed are service assets. Resources could be people, management, and their knowledge. In essence, every single aspect of a service is considered a service asset.

2. Risk Identification and Assessment

1. SKP shall ensure that risk assessments are undertaken to properly identify risks in line with the Company's assets. Risk assessments shall be based on an established framework for monitoring, escalation.
2. SKP shall ensure that Risk Assessment is performed before introducing new technology, information system, application to the Company's infrastructure
3. SKP shall ensure the Risk Assessment on all the business supporting IT Infrastructure, IT Assets, Network & Security devices, Data Center containing information servers, Applications, etc
4. Identified Risks shall be documented on the basis of identified threats and/or vulnerabilities and defined on the basis of its likelihood of such threats and impact on the business.
5. Risk owner shall be identified for all the risk, that is, the person responsible for mitigating the risk.
6. Risk Assessment shall be conducted considering the factors as Confidentiality, Integrity, and availability.

3. Process Identification

1. SKP shall identify all the processes and sub-processes for Risk Assessment and Treatment.
2. SKP shall identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality
3. The SKP shall identify all the information assets used for performing the identified business processes such as (a) Proprietary information belonging to the Company; (b) Personal information relating to employees; (c) Client information held; (d) All supplier, contractor and other third-party information; (d) All software assets; (e) All physical assets; (f) All services associated with the Company's information systems; (g) All external dependencies like service providers, third parties, etc.

4. Risk Treatment

1. **Risk Acceptance/Tolerance** - If the risk is too low, or within the risk threshold of the SKP, simply accept the risk. Management may also decide

to accept the risk if the mitigation measures are too expensive or too complex.

2. **Risk Reduction/Mitigation -** Reducing the vulnerabilities by putting preventive controls in place, and by reducing the threat impact with implementing more corrective/detective controls as deemed fit by the SKP.
3. **Risk Avoidance/Termination** Removing the threat completely.

5. Risk Mitigation

SKP shall implement appropriate internal security controls to mitigate risks pertaining to the Company's information assets. These controls shall be selected and implemented in compliance with this framework, and take into consideration:

1. Complying with requirements and managing constraints of the applicable national and international legislation and regulations.
2. Achieving the SKP strategic and financial objectives.
3. Managing operational requirements and constraints
4. Balancing the investment in implementation and operation of controls harm likely to result from security failures.

6. Reporting Risk Events

1. All the Risks Management activities shall be documented along with the Risk Assessment and Risk Treatment procedure, list of critical assets, threats and vulnerabilities associated with the critical assets.
2. Critical Assets shall be identified based on the Risk Identification process and should be used as per the guidelines defined in the Company's Acceptable Use Policy.

7. Reporting Information Security Events

1. SKP shall report known or suspected information security incidents to the Information Security (IS) Team.
2. If malware is suspected on a system, the user shall disconnect the system from the network immediately and notify their Information Security Team, and assist in removing the malware prior to re-connection with the network services.

3. All personnel shall cooperate with information security members in the investigation of the incident by providing accurate and timely information and active participation.
4. The incidents shall include information such as; (a) The unique ID of the Incident; (b) Incident Description; (c) Location and Date; (d) Severity (Prioritization of Incident); (e) Root Cause; (f) Correction; (g) Corrective action; (h) Current Status; (i) Impact
5. Only individuals in information security or audit role or an authorized designee by the information security shall test security weaknesses. The User is forbidden to test the security weakness without the permission, direction and involvement of the Information Security Team. The User shall not publicize the discovered vulnerability or weakness.

8. Management of Information Security Incidents

1. SKP Information Security Team shall provide coordination of the response and remediation of attacks on the Company's information assets. The Information Security Team is responsible for coordinating the response to system events throughout the Company information infrastructure, to include Third Party hosted systems, in an efficient, effective, and confidential matter.
2. Security incidents shall be reported to and investigated by the Information Security Team to determine the severity of the incident. Investigative methods and procedures will be used based upon the alert and incident levels defined in the information security procedures.
3. Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
4. Roles for members of the Information Technology (IT) Team for investigation shall be documented in IT operations procedures respectively.
5. A summary record of each incident should be maintained by the IT Team to document incident description, scope, actions are taken, closure, lessons learned, and any financial expenses related to the incident.

G. Cyber Security Preparedness Indicators.

SKP has developed indicators to assess the level of risk and/or preparedness to avoid a cyber security event. This includes spreading awareness among the stakeholders of the Company including its employees

1. **Network Segmentation Implementation -** Network segmentation necessitates classifying and categorizing IT assets, its data, and personnel into discrete groups, and then restricting access to these specific groups. By placing the resources into different areas of the network, a compromise for one sector or device shall not translate into the exploitation of the entire system.
2. **Secure Remote Access Usage** - The ability to connect remotely to a network such as a secure Virtual Private Network (VPN) may be used if remote access is entailed. A VPN is a secure encrypted data channel for sending and receiving data securely via public IT infrastructure.
   All critical systems over the internet should have two-factor security (such as VPNs, Firewall controls etc).
3. **Role Based Access Control -** Role-based access control permits or denies access to the network resources based on job functions. This hampers the ability of individual users or attackers to reach files or parts of the system they shouldn't access.
4. **Password Security** SKP shall use strong passwords for systems to maintain information security. Properties like changing of default password and use industry accepted best practices shall be established in the Company's password management document.
5. **Vulnerability Awareness and Patch Implementation** To protect the SKP from Cyber Security attacks, a system of monitoring, vulnerability assessment and applying system patches shall be implemented.
6. **Implement an Employee Cyber Security Training Program** When SKP employees aren't involved in Cyber Security, not only can vulnerabilities and threats go unnoticed, but the employees themselves may become conduits through which attacks are executed. Therefore, they should receive initial and periodic Cyber Security training, helping to maintain the security of the Company as a whole.

H. Cyber Crisis Management Plan

The Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism outlines a framework for dealing with cyber-related incidents for a coordinated, multi-disciplinary and broad-based approach for rapid identification, swift response, information exchange, and remedial actions to mitigate and recover from malicious cyber-related incidents impacting the critical business functions and processes of Company. Apart from this, other purposes are: -

1. To ensure that manipulations or interruption of critical functions/services cause the least possible damage.
2. To enable contingency plans in line with the Crisis Management Plan for countering cyber attacks and cyber terrorism, equip themselves suitably to implement, supervise the implementation and ensure compliance among all the organizational units within their domains.
3. To assist in order to place mechanisms for effectively dealing with cyber security crisis and to be able to pinpoint responsibilities and accountabilities right down to the individual level.

1. Types of Cyber Crisis

a. Large scale defacement and attacks on websites

Website defacement is a Defacer breaking into a web server and altering the contents of the website. Attackers may change the content of a web page subtly such that the alteration is not immediately apparent. As a result, false information is disseminated

b. Malware Attacks (Virus / Worm / Trojans / Botnets)

Malware or Malicious Code is software designed to infiltrate or damage a computer system without the owner's consent. The code is hostile, intrusive, or an annoying software/program code. Commonly known malware are worms, Trojans, virus, spyware, adware, and Bots.

c. Malware affecting Mobile devices

Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Android, iOS, Windows Mobile, Blackberry OS

d. Large scale SPAM attacks

Spamming is a misuse of the electronic messaging systems to indiscriminately send unsolicited bulk email messages. SPAM emails may also contain a virus, worm and other types of malicious software and are used to infect Information Technology systems.

e. **Large-scale spoofing**

Spoofing is an attack aimed at ‘Identity theft. Spoofing is a situation in which a program or a person successfully make-belief as another by falsifying data and henceforth gaining an illegitimate advantage.

f. **Phishing attacks**

A phishing attack is a type of attack which is aimed at stealing the ‘sensitive personal data’ that can lead to committing online economic frauds.

g. **Social Engineering**

It is the art of manipulating people into performing disclosure actions or divulging confidential information.

h. **Infrastructure attacks**

Attacks such as D DoS, DoS, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralized / Distributed Control System (DCS), Gateways of ISPs and Data Networks, Infection of Programmable Logic Control (PLC) systems by sophisticated malware

2. Points for Action

The following points of actions shall be taken in correspondence with the cyber crises.

a. Identification of key information and technology assets that support the services of that organization Implementation of controls to protect those assets from cyber attack.
b. Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption.
c. Periodically test the effectiveness of technical control security, especially after any significant change to the IT applications, systems or networks which may include
(i). Vulnerability assessment (ii) Penetration testing (iii) Application security testing (iv) Web security testing
d. To ensure identification, prioritization, assessment, remediation, and protection of organization infrastructure and key resources.

e. To carry out periodic mock drills based on the criticality of the application or infrastructure.

I. Reporting of Information on Cyber Security

The objective is to have a suitable mechanism in place to report all types of unusual security incidents to its Internal Technical Committee to deal with incidents involving compromise of IT systems of the Company such as data breach, data destruction, etc. which has a severe impact on the Company's operations

1. Cyber Security Incident

It is an event which appears to be a breach of Company's Cyber Security implemented controls, which may lead to loss of confidentiality, integrity, and availability of information systems. This can lead to

a. Denial of Service
b. Unauthorized access
c. Virus, worm, and trojan horse attack
d. Loss of confidentiality, integrity, and availability of information systems.

2. Recording and Incident Handling

The recording and the handling of the Cyber Security incident shall be done by the SKP Cyber **Crisis Management** Team.

a. Cyber Crisis Management Plan Team shall log, categories and prioritize all cyber security incidents.
b. If an incident is classified as critical, the team will check whether disaster recovery action is required.

3. Cyber Incident Logging

SKP Cyber **Crisis Management** Team shall ensure that the below details are captured for each Cyber Security incidents, but not limited to (i).The unique ID of the incident (ii) Incident description (iii) Location and date (iv) Category and incident severity (v) Root cause analysis (vi) Corrective action taken (vii) Impact of the Incident including data loss/leakage or destruction.

J. Vulnerability and Patch Management

Information Security officer is responsible for conducting a Vulnerability Management Program to identify, assess and patch the vulnerabilities in Company Network, Information Systems, and Applications.

Information Security Officer is responsible for posting security advisories for all Users who may be affected by security issues. Security advisories should include warnings on specific risks including issues such as viruses, social engineering, new technical vulnerabilities, and the Company specifics risks and counter measures.

Publicly available systems including websites and web-based applications should be coded and tested for security vulnerabilities and patched so that no high-risk vulnerability remains in the system.

a. Technical Vulnerability Management

Information Security Officer should compile and maintain records of all information assets owned by the Company. Security and vulnerability information should be obtained and evaluated for applicability to the software and technology currently in use. SKP shall regularly conduct Vulnerability Management Program to detect security vulnerabilities in the IT environment along with the periodic penetration tests, at least once in a year, in order to conduct an evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. Internal and external vulnerability scans for the network, information systems and applications should be conducted **every year or half yearly** for critical systems as a part of the Vulnerability Management Program.
Mitigating actions should be taken if software patches or fixes do not exist for identified technical vulnerabilities. These actions include: (i) Disabling services (ii) Modifying security architecture components (iii) Increased monitoring of the vulnerability.

b. VAPT prior to the commissioning of a new system

Vulnerability Assessment and Penetration Testing should be carried out prior to the commissioning of a new system or application to a Company's infrastructure which offers internet access and open network interfaces. Information Security Officer is responsible for conducting a Vulnerability Management Program prior to the commissioning of a new system.

c. VAPT after any significant change

Internal and external Vulnerability scans and Penetration Tests should be conducted after any significant change to the network, information systems, and applications. Information Security.

d. Patching

All information system components and software shall be protected from known vulnerabilities by installing applicable patches at defined intervals which includes the identification, categorization and prioritization of patches. It shall also include an implementation for each category of patches to be applied in a timely manner.

Information Security Officer should ensure that the patches are installed for all the vulnerabilities identified in the VAPT. No system and/or Application should contain a High level of vulnerability.

e. Reporting Security Weaknesses

If a User suspects a security weakness, threat or System vulnerability, that individual should notify the Information Security Officer. The User is forbidden to test the security weakness without the permission, direction, and involvement of the Information Security Officer. The User should not publicize the discovered vulnerability or weakness.

f. VAPT Result Records

All the records of the Vulnerability Management Program should be kept along with the vulnerabilities identified and patches applied to these vulnerabilities. IS Officer is responsible for maintaining the records of Vulnerability Management Programs.

K. Cyber Security Awareness

An Information Security Awareness program must be organized at least once a year to including, but not limited to:

(i).Awareness of ISMS Policy (ii) Password Security (iii) Two-factor authentication (iv) Phishing (v) Fake Emailing and verification of email source (vi) Spam Filtration (vii) Social Engineering Attacks (viii) Cyber Crimes (ix) Information Disclosure on social media and other websites (x) Malicious websites and threats from them (xi) Data backup and storage (xii) Incident reporting and response

L. Access Management

a. No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.
b. Any access to the SKP systems, applications, networks, databases, etc. shall be for a defined purpose and for a defined period. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
c. SKP shall implement an Access Management policy which addresses strong password controls for users' access to systems, applications, networks and databases in line with **Annexure C** of this Policy.
d. All critical systems of the Company accessible over the internet should have a two-factor authentication mechanism implemented
e. The Company shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.
f. SKP shall deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stock Broker / Depository Participant's critical systems. Such controls and measures should inter-alia include 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.

g. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the SKP critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.
h. SKP shall formulate 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.
i. User Management must address deactivation of access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

M. Physical Security

a. 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.
b. Physical access to the critical systems should be revoked immediately if the same is no longer required
c. SKP shall ensure that the perimeter of the critical equipment room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards,
CCTV, card access systems, mantraps, bollards, etc. where appropriate.

N. Network Security Management

SKP establishes 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 Company's premises with proper access controls.

For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications. SKP 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 must be deployed to address virus / malware / ransom ware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.

O. **Data security**

Critical data must be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B.

1. SKP shall implement measures to prevent unauthorized access or copying or transmission of data/information held in a contractual or fiduciary capacity. It should be ensured that the confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. SKP shall ensure security during transportation of data over the internet as per Annexure B of this policy

2. The **information security policy** should also cover 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.

3. SKP shall allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.

4. SKP shall only deploy hardened hardware/software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for of the system.

5. Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures are taken to secure them.

P. Application Security in Customer Facing Applications & Patch management

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. An illustrative list of measures for ensuring security in such applications is provided in **Annexure C**.

The Company shall ensure that off the shelf products being used for core business functionality (such as Back office applications) bears Indian Common criteria certification of Evaluation Assurance Level 4. By Standardisation Testing and Quality Certification (STQC).

The Custom developed / in-house software and components shall not obtain the certification. However, they shall have an intensive regression testing, configuration testing as per Company's Software Testing process which includes the business logic and security controls.

SKP should establish and 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.

SKP should 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.

Q. Disposal of data, systems and storage devices

The critical data and/or information on such devices and systems shall be removed by using methods such as crypto shredding or physical destruction, as applicable.

R. Monitoring and Detection & Response and Recovery

SKP 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 and/or 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 anomalies.

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

S. BCP and DR

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.

SKP should have timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Stock Brokers / Depository Participants should 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.

SKP 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.

SKP should also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

T. Compliance

All requirements specified in this Cyber Security and Cyber Resilience framework must be adhered by all the users and managed by the Company's internal Technology Committee.

Quarterly reports containing information on cyber-attacks and threats experienced 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.

In case, the systems such as IBT, Back office, Customer facing applications, IT infrastructure, etc. of the SKP are managed by vendors, the SKP 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.

The Company shall undergo an annual periodic audit w.r.t. vide circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013, shall accordingly stand modified to include audit of implementation of the aforementioned areas.

In reference to the SEBI circular Dated 30th June 2022 circular no - SEBI/HO/MIRSD/TPD/P/CIR/2022/93 any 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. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in. 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.

In reference to the SEBI circular No - SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated – 07th June 2022 -

Stock Brokers / Depository Participants shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board/Partners/Proprietor of the Stock Brokers / Depository Participants shall approve the list of critical systems. Stock Brokers / Depository Participants 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.

Stock Brokers / Depository Participants 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 Stock Brokers / Depository Participants etc., 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. The VAPT test shall conduct VAPT at least once in a financial year. 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.

U. Review

The Policy shall be approved and reviewed by the Board / Partners / Proprietor of the Stock Broker / Depository Participants on an annual basis. However, any minor change(s) to the Company's policy due to a modification in the Cyber Security and Cyber Resilience framework as given by SEBI and/or Company's Infrastructure may be proposed by the Company's "Internal Technology Committee" and shall be placed before the Board / Partners / Proprietor of the Stock Brokers / Depository Participants for appropriate action.

The Internal Technology Committee shall, on half yearly basis, review the implementation of the Cyber Security and Cyber Resilience policy which includes reviewing current IT and Cyber Security and Cyber Resilience capabilities, setting goals for a target level of Cyber Resilience, and establishing plans to improve and strengthen Cyber Security and Cyber Resilience of the Company.

V. Exception

In case, 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. The Company, in that case, is not responsible for applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

Annexure - A

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 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. Analyze 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.

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 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.

Annexure C

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 smart phones 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 e-mail and phone number) is 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

Place : Kolkata
Date : 10/07/2022