CORUM SECURITIES PRIVATE LIMITED

50/6A, Harish Mukherjee Road, Kolkata - 700 025
Tel.: 033 2454 0021 / 10 / 44, Fax : 033 2454 8177
E-mail : ID for Investor Grievance : info@corumsecurities.com, jiteshgandhi@corumsecurities.com
CIN - U67120WB2002PTC094505

CORUM SECURITIES PVT LTD

INFORMATION SECURITY POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	02/01/2024
Policy Approved by	Board of Directors
Policy approved on	02/01/2024

Version – 1.2

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this Policy is to safeguard information belonging to the Company and its stakeholder (third parties, clients or customers and the general public), within a secure environment.

This Policy informs the Company's staff, and other external Vendors entitled to use Company facilities, of the principles governing the holding, use and disposal of information.

It is the goal of the Company that:

- Information will be protected against unauthorised access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Director of ICT Systems, and investigated through the appropriate management channel.

Information relates to:

Electronic information systems (software, computers, and peripherals) owned by the Company whether deployed or accessed on or off campus.

The Company's computer network used either directly or indirectly.

Hardware, software and data owned by the Company.

Paper-based materials.

Electronic recording devices (video, audio, CCTV systems).

The Policy

The Company requires all users to exercise a duty of care in relation to the operation and use of its information systems.

Authorised users of information systems

- With the exception of information published for public consumption, all users of Company information systems must be formally authorised by appointment as a member of staff, or by other process specifically authorised by the designated officer. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network password policy" describes these principles in greater detail.
- Authorised users will pay due care and attention to protect Company information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:
  - permission of the information owner

- the risks associated with loss or falling into the wrong hands
- How the information will be secured during transport and at its destination.

Acceptable use of information systems

- Use of the Company's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of subsidiary policies.

Information System Owners

- Designated Officer/Chief Technology Officer/Directors who are responsible for information systems are required to ensure that:
  - Systems are adequately protected from unauthorised access.
  - Systems are secured against theft and damage to a level that is cost-effective.
  - Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
  - Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
  - Data is maintained with a high degree of accuracy.
  - Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
  - Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
  - Any third parties entrusted with Company data understand their responsibilities with respect to maintaining its security.

Personal Information

- Authorised users of information systems are not given rights of privacy in relation to their use of Company information systems. Duly authorised officers of the Company may access or monitor personal data contained in any Company information system (mailboxes, web access logs, file-store etc.).
- Individuals in breach of this policy are subject to disciplinary procedures at the instigation of the Designated Officer with responsibility for the relevant information system, including referral to the Police where appropriate.
- The Company will take legal action to ensure that its information systems are not used by unauthorised persons.

Ownership

- The Designated Officer of ICT Systems has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.
- Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For M/s. Corum Securities Pvt. Ltd

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

(Jitesh Dineshchandra Gandhi)

Designated Director

Dated: - 02/01/2024

CORUM SECURITIES PRIVATE LIMITED

50/6A, Harish Mukherjee Road, Kolkata - 700 025
Tel.: 033 2454 0021 / 10 / 44, Fax : 033 2454 8177
E-mail : ID for Investor Grievance : info@corumsecurities.com, jiteshgandhi@corumsecurities.com
CIN - U67120WB2002PTC094505

CORUM SECURITIES PVT LTD

ELECTRONIC STORAGE MEDIA DISPOSAL POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	02/01/2024
Policy Approved by	Board of Directors
Policy approved on	02/01/2024

Version – 1.2

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this policy is to define standards for proper data sanitization and/or disposal of electronic storage media that has (or may have) contained personal information at the Company's end and to emphasize the importance of protecting sensitive information and complying with legal and regulatory requirements during the disposal of electronic storage media.

General/Definitions

- **Electronic Storage Media** – Any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.

- **Personal information** – An individual's first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver's license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personally identifiable identification number or password, that would permit access to a resident's financial account.

- **Sensitive Information** – Data whose disclosure would not result in any business, financial or legal loss but involves issues of personally identifiable credibility, privacy or reputation. The security and protection of this data is dictated by a desire to maintain staff and student privacy.

- **Sanitizing Storage Media** –
  - Disposal is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.
  - Clearing is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.
  - Purging is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory process. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Policy, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of Purging electronic storage media
  - Destroying is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for

single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.

Data Wiping –

Identify the Media: Clearly identify the electronic storage media that needs to be wiped. Ensure that you are working with the correct device.

Backup Important Data: Before initiating the data wiping process, backup any important data if necessary. Ensure that critical information is securely stored elsewhere.

Disconnect from Network: Disconnect the electronic storage media from any network connections to prevent remote access during the wiping process.

Choose Wiping Method: Select an appropriate wiping method based on the type of storage media. Common methods include overwriting, cryptographic erasure, or using specialized software tools. Choose a method that complies with your organization's security policies.

Use Certified Software: If using software for data wiping, ensure that it is certified and recognized for secure data erasure.

Follow Software Instructions: If using a software tool, follow the step-by-step instructions provided by the software vendor. This may involve creating a bootable disk or USB drive, selecting the target storage media, and initiating the wiping process.

Verify Completion: After the wiping process is complete, use the software's verification features to ensure that all data has been successfully erased. Some tools provide a certificate or report confirming the completion of the process.

Physically Label or Tag: Physically label or tag the wiped media to indicate that it has undergone the data wiping process. This helps in tracking and inventory management.

Record Details: Maintain a record of the data wiping process, including the date, time, method used, and any relevant details. This documentation may be required for compliance purposes.

Secure Storage or Disposal: If the storage media will be reused, store it securely. If it will be disposed of, follow the organization's disposal procedures, ensuring that it is done securely and in compliance with environmental regulations.

Consider Cryptographic Erasure for SSDs: For SSDs, consider using cryptographic erasure methods that leverage the built-in encryption features of the device. This can be more effective than traditional overwriting methods.

Organizational Scope

This policy applies to all personnel who have responsibility for the handling and proper disposal of electronic storage media at Company.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Policy Content and Guidelines

- All electronic storage media should be sanitized (Cleared/Purged) prior to sale, donation, being moved to unsecured storage (for spare parts), or transfer of ownership. A transfer of ownership may include transitioning media to another individual or department at the Company or replacing media as part of a lease agreement.

- All electronic storage media must be destroyed when it has reached the end of its useful life and/or when other sanitizing methods are not effective (e.g. single-write media or media that is permanently write protected), provided that the destruction does not conflict with Company data retention policies or any regulatory requirements (e.g. electronic discovery).

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For M/s. Corum Securities Pvt. Ltd

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

(Jitesh Dineshchandra Gandhi)

Designated Director

Dated: - 02/01/2024

CORUM SECURITIES PRIVATE LIMITED

50/6A, Harish Mukherjee Road, Kolkata - 700 025
Tel.: 033 2454 0021 / 10 / 44, Fax : 033 2454 8177
E-mail : ID for Investor Grievance : info@corumsecurities.com, jiteshgandhi@corumsecurities.com
CIN - U67120WB2002PTC094505

CORUM SECURITIES PVT LTD

DATA LEAKAGE POLICY

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	Designated Officer
Policy reviewed by	Technology Commitee
Policy reviewed on	02/01/2024
Policy Approved by	Board of Directors
Policy approved on	02/01/2024

Version – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

This policy is a guide in identifying and gaining an understanding of the components that make up the information security system to manage risk to systems, assets, data, and capabilities.

Scope

Data Leakage Policy (DLP) is a set of technologies and business policies to make sure end-users do not send sensitive or confidential data outside the organization without proper authorization. DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Sensitive information might include financial records, client data, credit card / debit card data, or other protected information. The most common method that this data is leaked is via email.

Policy

Data Leakage Policy (DLP) features and products enable your organization to locate, monitor and protect your sensitive content from loss or misuse. Through policy enforcement, the organization will be complying by minimizing risk and preventing unauthorized use of confidential information.

Data Leakage Policy (DLP) encompasses the processes and rules used to detect and prevent the unauthorized transmission or disclosure of confidential information. The purpose of this procedure is to establish a framework of controls for classifying and handling the organization's data based on the data's level of sensitivity, storage location, value, etc. Confidential data can reside on or in a variety of mediums (pictures, paper documents, shred bins, physical servers, virtual servers, databases, file servers, personal computers, point-of-sale devices, USB drives and mobile devices) and can move through a variety of methods (human, network, wireless, etc.). The organization relies on a variety of DLP strategies and solutions to prevent data loss. The organization's DLP strategies and solutions are reevaluated regularly to ensure their relevancy and effectiveness. This security procedure applies to all the employees and users of the organization. Individuals working for the organization internally or externally are subject to the same rules when they are using the organization's information technology resources or have any means of access to data that has been classified as confidential or private.

- **Best Practices**
  - The sender will receive an Outlook message when an email is sent that contains sensitive information. Faculty and staff can still manually encrypt any email.
  - Do not forward email you receive that contains sensitive information. If it is required to do so, redact the sensitive information before replying.
  - Seek alternate means of transmitting the sensitive data. (secure web applications, etc.)

- **Data classification**

In the context of information security, is the classification of data based on its level of sensitivity and the impact to the organization should that data be disclosed, altered or destroyed without authorization. Classification of data will aid in determining baseline security controls for the protection of the data. All organizational data is classified into one of three sensitivity levels (tiers), or classifications:

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Tier 1-

Confidential Data i.e., when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the organization. Unauthorized access to or disclosure of confidential information could constitute an unwarranted invasion of privacy and cause financial loss and damage to the organization's reputation and the loss of community confidence. The highest level of security controls should be applied. Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the organization who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be requested for an individual and approved by the Technology Committee. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data.

Restricted Data is a particularly sensitive category of Tier 1-Confidential data. Restricted data is defined as 'any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transmission'.

Tier 2-

Internal/Private Data i.e., when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the organization. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data. Access to Internal/Private data must be requested for an individual and approved by the Technology Committee. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data. Access to Internal/Private data may also be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department. Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the organization should this information not be available when needed is typically moderate. Examples of Internal/Private data include such as financial reports, some research data.

Tier 3-

Public Data i.e., when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the organization. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data. Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected.

Violations –

Anyone who knows or has reason to believe that another person has violated this procedure shall report the matter promptly to his/her supervisor, department head or the Technology Committee. After a violation of this procedure has been reported or discovered, the issue will be handled as soon as possible to reduce harm to the organization. Violators of this procedure may be subject to disciplinary action, up to and including the termination of employment depending on the severity of the violation or data breach.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For M/s. Corum Securities Pvt. Ltd

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

(Jitesh Dineshchandra Gandhi)

Designated Director

Dated: - 02/01/2024

CORUM SECURITIES PRIVATE LIMITED

50/6A, Harish Mukherjee Road, Kolkata - 700 025
Tel.: 033 2454 0021 / 10 / 44, Fax : 033 2454 8177
E-mail : ID for Investor Grievance : info@corumsecurities.com, jiteshgandhi@corumsecurities.com
CIN - U67120WB2002PTC094505

CORUM SECURITIES PVT LTD

POLICY ON CYBER SECURITY AND CYBER RESILIENCE

Circular: - Ref. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	02/01/2024
Policy Approved by	Board of Directors
Policy approved on	02/01/2024

Version – 1.3

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Introduction

Our organization is a leading financial institution specializing in stock broking and depository participant services. Established [F.Y. -2023-24], we have emerged as a trusted partner in the financial market, providing comprehensive solutions to our clients.

- **Vision and Mission:**
  - **Vision:** To be a preferred choice for investors seeking reliable and innovative financial services.
  - **Mission:** To deliver exceptional value through cutting-edge technology, ethical practices, and customer-centric services.
- **Services:**
  - Stock Broking:
    - Equities Trading
    - Derivatives Trading
    - Currency Trading
    - Commodities Trading
  - Depository Participant Services:
    - Dematerialization (Demat) of Securities
    - Account Maintenance
    - Electronic Settlement of Trades
- **Technology Infrastructure:** We leverage state-of-the-art technology to ensure seamless and secure trading experiences for our clients. Our robust trading platforms and advanced risk management systems contribute to the efficiency of our operations.
- **Regulatory Compliance:** As a registered stock broker and depository participant, we adheres to all regulatory requirements mandated by SEBI/Exchange(s)/Depository(s). We prioritize transparency and compliance in all our dealings.
- **Clientele:** Our diverse clientele includes retail investors, corporates. We are committed to understanding and addressing the unique financial needs of each client.
- **Awards and Recognition:** Our organization has received accolades for its excellence in the financial services industry. These recognitions underscore our commitment to delivering top-notch services.
- **Contact Information:** For inquiries or to learn more about our services, please contact us at: [50/6A, Harish Mukherjee Road, Kolkata - 700025] [Phone: 033 24540021] [Email: info@corumsecurities.com] [Website: www.corumsecurities.in]
- **Social Responsibility:** Our organization is dedicated to social responsibility and community development. We actively participate in initiatives that contribute to the welfare of society.

Background

SEBI has issued circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019, SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68

ed May 20, 2022, SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022 and EBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023 providing guidelines on Cyber Security and Cyber Resilience. The objective of the said circular is to adapt to the rapid technological developments in Securities Market which have highlighted the need for robust Cyber and Cyber Resilience at the level of Stock brokers/Depository participants who are performing significant functions in providing services to the holder of Securities.

In order to protect the integrity of data and guard against breaches of Privacy and to comply with the applicable regulations our organization has framed a policy for implementation to meet the objectives.

Date of Implementation of the Circular

Circular shall be effective from April 1, 2019.

It is observed that the level of Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber 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

Accordingly, the following Policies & Procedures have been put in place

Governance

Risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats.

- Identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:
  - 'Identify' critical IT assets and risks associated with such assets.
  - 'Protect' assets by deploying suitable controls, tools and measures.
  - 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
  - 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
  - 'Recover' from incident through incident management and other appropriate recovery mechanisms.

- As a Stock broker trading through APIs based terminal or acting as a depository Participants should refer best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

  - ISO 27001 is an international standard for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System. The standard is a joint effort by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).
  - COBIT 5 is a framework from the Information Systems Audit and Control Association (ISACA) for the management and governance of information technology (IT). ... Achieve strategic goals by using IT assistance. Maintain operational excellence by using technology effectively. Keep IT-related risk at an acceptable level.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

- The main benefit of implementing ISO 27001 is a systemic Information Security Management System that helps with the identification of critical information, the information security risk assessment of the system, and the implementation of security controls, all of which help to create a secure culture in the organization.
- ISO 27001 is beneficial for the organization in terms of its security.
- The five COBIT 5 principles are:
  - Meeting stakeholder needs
  - Covering the enterprise end to end
  - Applying a single integrated framework
  - Enabling a holistic approach
  - Separating governance from management

- We have designated Mr. **Jitesh Dineshchandra Gandhi** .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.
- A reporting procedure has been designed to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.
- The Designated officer and the technology committee will periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

- The technology committee are consisting of following members:

Sl. No.	Designation of the Members	Name of the Committee Members
1	CISO (Chief Information Security Officer)	Jitesh Dineshchandra Gandhi
2	Designated Officer	Jitesh Dineshchandra Gandhi
3	IT Head	Jitesh Dineshchandra Gandhi
4	Compliance Head	Jitesh Dineshchandra Gandhi
5	Any other employee(s) indulges in IT	Jitesh Dineshchandra Gandhi

Identification

- We have identified and classified / designated critical assets based on their Sensitivity and criticality for business operations, services and data management. The critical assets 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 are classified as critical system. Maintenance of up-to-date inventory of the hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

flows. Accordingly identify cyber risks, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

- To this end, our organization is maintaining 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.

Protection

Access controls:

- Any access to systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. To identify the access we have granted access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.
- 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, should be subject to stringent Supervision, monitoring and access restrictions.

Physical Security:

- Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees. Access should be revoked immediately if the same is no longer required.
- Office premises should be physically secured and monitored by security guards.

Network Security Management:

- As a Stock Brokers / Depository Participants we have established 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 should be secured within the premises.
- Adequate controls must be deployed to address virus / malware / ransom ware attacks.

Data security:

- Strong encryption methods to be used for identifying and encrypting the critical data. The confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc.

Hardening of Hardware and Software:

- Should 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 should be blocked.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Application Security in Customer Facing Applications: Application security for Customer facing applications offered over the Internet such as IBTs, portals containing sensitive or private information and Back office applications are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. Measures to be taken for applications.

Patch management:

- Patch management procedures should 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. Testing to be performed on 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.

Disposal of data, systems and storage devices:

- Identify a Policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

Vulnerability Assessment and Penetration Testing (VAPT):

- We will carry out periodic vulnerability assessment and penetration testing (VAPT) which inter-alia includes all critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems 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.
- We will conduct VAPT at least once in a financial year. However, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC), VAPT shall be conducted at least twice in a financial year. Further, only CERT-In empanelled organizations are required to engage for conducting VAPT.
- The final report on said VAPT should be submitted to SEBI after approval from Standing Committee on Technology (SCOT), within 1 month of completion of VAPT activity.
- Any gaps/vulnerabilities detected have to be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report to SEBI. In addition, we should also 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. Systems which are publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.

Monitoring and Detection:

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

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 should also be monitored for anomalies.

- Ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.

Response and Recovery:

- Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of Cyber-attack or breach, mitigate its effect and eradicate the incident.

- The response and should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. 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.

Sharing of Information:

- All 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 June, September, December and March of every year.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

ıining and Education

Entities should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.

- The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Systems managed by vendors, MIIs

- As a Stock Brokers / Depository Participants we have instructed the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

Periodic Audit

- The periodicity of audit for the purpose of compliance with Cyber Security and Cyber Resilience provisions for depository participants shall be annual.
- The periodicity of audit for the compliance with the provisions of Cyber Security and Cyber Resilience provisions for stock brokers, irrespective of number of terminals and location presence, shall be as under: (Type of stock broker as specified in SEBI circular CIR/MRD/DMS/34/2013 dated November 06, 2013)
    - For Type I - Annual
    - For Type II - Annual
    - For Type III - Half-year.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

- Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.
- Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.

- **Privilege Management:**
  - Maker-Checker framework should be implemented for modifying the user's right in internal applications.
  - For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.
- **Cybersecurity Controls:**
  - Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
  - Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.
  - Restrict execution of "PowerShell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
  - Utilize host-based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
  - Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.
- **Security of Cloud Services:**
  - Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
  - Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.
  - Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.
  - Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.
- **Implementation of CERT-In/ CSIRT-Fin Advisories:**

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India:

- Protection of Critical Information Infrastructure (CII) is of paramount concern to governments worldwide. To address this threat, the Government of India has notified the 'National Critical Information Infrastructure Protection Centre' (NCIIPC) as the nodal agencies vide Gazette of India notification on 16th January 2014.
- NCIIPC is driven by its mission to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country. To achieve this, it is essential to ensure that relevant security mechanisms are built into Critical Information Infrastructure as key design features.
- The National Security Advisor had in July 2013 released a document listing forty controls and corresponding guiding principles for the protection of CIIs. In view of the dynamic nature of cyberspace and to ensure the continued relevance of these controls, NCIIPC is continuously reassessing these based on ongoing experience as well as feedback from NCII constituents, these controls have been grouped into five sets (or families). While all Controls in a family may not be relevant to a particular organization / infrastructure, it is important that conscious sign off (on both, controls implemented, as well as dropped) is taken from senior management based on residual risk acceptable to the Organization.

- **The five families of controls are:**
  - Planning Controls for ensuring that the security is taken as a key design parameter for all new CIIs at conceptualization and design level itself.
  - Implementation Controls for translating the design/conceptualization planning into mechanisms for protecting the CII. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.
  - Operational Controls for ensuring that the desired security posture is maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected / poorly protected CII.
  - Disaster Recovery/ Business Continuity Planning (BCP) Controls for ensuring minimum downtime and the restoration process.
  - Reporting and Accountability Controls for ensuring adequate accountability and oversight exercised by Senior management, as well as reporting to concerned Government agencies where required enforced through compliance controls.
  - In circumstances where a particular control may not provide the best fit, we as an organization needs to consider compensatory controls which could also be procedural, so as to ensure that the attack surface presented by the organization's Information Infrastructure is minimized.

Advisory for Stockbroker – Member onboarding for CERT-In Cyber Swachhta Kendra (CSK):

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

recent times, there has been a surge in cyber-attacks in organizations across the globe impacting the continuity of heir business operations and causing sensitive data leakage through malware infections at end point computing devices. To mitigate such malware and botnet infections, CERT-In has launched an initiative named '**Cyber Swachhta Kendra**' (CSK), which provides information and enables organizations to disinfect the computing devices using free-of-cost malware and botnet cleaning tools.

Compliance Requirement:

Organization having more than 50,000 active traded clients and also providing Internet Based Trading platform are required to onboard themselves on 'Cyber Swachhta Kendra'

Other members (not part of the above criteria) can also voluntarily subscribe to the services and avail actionable information intelligence from CSK.

For receiving the reports/alerts from Cyber Swachhta Kendra on daily basis, Organization is required to follow the guidelines for onboarding on Cyber Swachhta Kendra Portal.

Organization can communicate with CERT-In Cyber Swachhta Kendra through email address "csk@cert-in.org.in" and contact number 1800-11-4949 can also be used as an alternative.

Illustrative Measures for Data Security on Customer Facing Applications

Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is dee med absolutely necessary is transmitted and displayed.

Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank accoun t 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 som ething akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piec e of data over various networks

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.

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.

Use industry standard, strong encryption algorithms (e.g.: RSA, AES etc.) wherever encryption is implemented. It is important to identify datathat 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.

Ensure that all critical and sensitive data is adequately backed up, and that the backup locationsare adequately secured. For inst ance, on servers on isolated networks that have 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.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For M/s. Corum Securities Pvt. Ltd

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

(Jitesh Dineshchandra Gandhi)

Designated Director

Dated: - 02/01/2024