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

WFH ENVIRONMENT POLICY

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 – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this Work from Home (WFH) Policy is to provide guidelines and procedures for employees at our Company, when working remotely. This policy aims to ensure productivity, data security, and the well-being of employees in a WFH environment.

Scope

This policy applies to all employees who have been authorized to work remotely on a temporary or permanent basis.

Eligibility and Approval

Eligibility Criteria

- Employees eligible for WFH arrangements will be determined based on job responsibilities and performance.
- Not all positions may be eligible for remote work.

Approval Process

- Requests for WFH arrangements must be submitted to the employee's supervisor and approved by the respective department head or HR.
- Approvals will be based on business needs and the employee's ability to meet performance expectations remotely.

Work Hours and Availability

Work Hours

- Employees are expected to adhere to their regular work hours unless alternative arrangements are approved.
- Flexibility in work hours may be granted based on business needs and mutual agreement.

Availability

- Employees must be available during agreed-upon working hours and remain reachable through approved communication channels.
- Communication about unavailability must be communicated in advance.

Home Office Setup

Equipment and Technology

- Employees are responsible for providing their own equipment, such as laptops, monitors, and internet connectivity.
- The IT department will provide necessary support and guidelines for setting up a secure home office.

Data Security

- Employees must ensure the security of company data by using secure networks, encrypted connections, and following data protection policies.
- Devices used for work must be password-protected and kept in a secure environment.

Communication and Collaboration

- Employees must use approved communication and collaboration tools for work-related activities.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

- Employees will be responsible for their own internet and utility costs.
- Reimbursement for business-related expenses may be considered on a case-by-case basis.

Health and Well-being

- Employees are encouraged to take regular breaks, maintain a healthy work-life balance, and communicate any concerns about well-being.
- Ergonomic guidelines will be provided for setting up a comfortable workspace.

Security Awareness Training

Employees will undergo security awareness training to recognize and address cybersecurity threats in a remote work environment.

Termination of WFH Arrangements

- WFH arrangements may be terminated based on business needs or if there is a violation of company policies.
- Notice will be given, and a discussion will be held before terminating WFH arrangements.

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 REPORTING OF UNUSUAL ACTIVITIES

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 – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this policy is to establish guidelines and procedures for reporting unusual activities at our Company. This policy aims to encourage employees to promptly report any suspicious or irregular activities that could potentially impact the firm's operations, regulatory compliance, or the integrity of financial markets.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have knowledge of or suspect unusual activities within the stock brokerage firm.

Definitions

Unusual Activities

Any activity that deviates from the normal or expected behaviour and may indicate potential risks, fraud, or regulatory non-compliance.

Reporting Party

Individuals who witness or have knowledge of unusual activities and are responsible for reporting such activities.

Reporting Process

Identification of Unusual Activities

Employees are encouraged to be vigilant and promptly report any unusual activities they observe or become aware of during the course of their duties.

Reporting Channels

- Unusual activities can be reported through designated reporting channels, including but not limited to:
  - Direct supervisors or managers
  - Compliance department
  - Internal audit
  - Whistle-blower hotline or reporting platform

Anonymous Reporting

To encourage transparency, the firm provides anonymous reporting options, such as a confidential hotline or online reporting system.

Whistle-blower Protection

The firm is committed to protecting whistle-blowers from retaliation and ensuring confidentiality to the extent permitted by law.

Investigation Process

Designated Investigation Team

An investigation team will be designated to assess and investigate reported unusual activities promptly.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Confidentiality

Information related to the reported unusual activities will be treated with the utmost confidentiality during the investigation process.

Communication

Regular updates on the status of investigations will be communicated to the reporting party to the extent possible without compromising the investigation.

Non-Retaliation

The firm strictly prohibits retaliation against any individual who, in good faith, reports unusual activities. Retaliation is a violation of company policy and may result in disciplinary action.

Training and Awareness

Employees will receive training on recognizing and reporting unusual activities as part of their compliance and ethics training.

Compliance and Legal Considerations

Regulatory Compliance

The reporting process will comply with relevant financial regulations and industry standards.

Documentation

Detailed records of reported unusual activities, investigations, and outcomes will be maintained for compliance and audit purposes.

Review and Update

This policy will be reviewed regularly and updated as necessary to address changes in regulations, business processes, and emerging risks.

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 DISPOSAL AND RETENTION POLICY:

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 detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified the retention and disposal policy refers to both hard and soft copy documents. This Policy is also for the purpose of aiding employees in understanding their obligations of retaining electronic documents - including email, text files, digital images, sound and movie files, PDF documents, and all Microsoft Office or other formatted files or paper documents.

Review:

This policy defines the Data retention and destruction schedule for paper and electronic records. The Data Retention Schedule is approved as the initial maintenance, retention and disposal schedule for the physical (paper) and electronic records. The Technology committee of Company is responsible for the administration of this policy and the implementation of processes and procedures. In continuation with SEBI guidelines, the Designated Officer is also authorized to; make modifications to the Record Retention Schedule as needed to ensure that it is in compliance with SEBI regulations; ensure the appropriate categorization of documents and records on behalf of the company annually review the policy; and monitor compliance with this policy. Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

How long we should keep our paper records -

- ✓ Records should be kept for as long as they are needed to meet the operational needs of the Authority, together with legal and regulatory requirements. We have assessed our records to:
  - Determine their value as a source of information about the Authority, its operations, relationships and environment
  - Assess their importance as evidence of business activities and decisions
  - Establish whether there are any legal or regulatory retention requirements
- ✓ Where records are likely to have a historical value, or are worthy of permanent preservation, we will transfer them to the National Archives after 25 years.

Responsibilities of Employees –

All employees are responsible for:

- ✓ checking that any information that they provide in regards to their employment is accurate and up to date.
- ✓ informing the regulatory authority of any changes to information, which they have provided i.e. changes of address
- ✓ Checking the information that the Organization will send out from time to time, giving details of information kept and processed about employees.
- ✓ Informing Designated Officer of any errors or changes. The Company cannot be held responsible for any errors unless the employees has informed the management of them.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Disposal schedule:

- ✓ A disposal schedule is a key document in the management of records and information.
- ✓ Records on disposal schedules will fall into three main categories:

- Destroy after an agreed period – where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 3 years; destroy 2 years after the end of the financial year).
- Automatically select for permanent preservation – where certain groups of records can be readily defined as worthy of permanent preservation and transferred to an archive.
- Review is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

✓ Records can be destroyed in the following ways:

- **Destruction**
  - Non-sensitive information – can be placed in a normal rubbish bin
  - Confidential information – cross cut shredded and pulped or burnt
  - Highly Confidential information – cross cut shredded and pulped or burnt

✓ Electronic equipment containing information - destroyed using kill disc and for individual folders, they will be permanently deleted from the system.

✓ Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

✓ Archival transfer

- This is the physical transfer of physical records to a permanent custody at the National Archives Office.

Sharing of information:

✓ Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines mentioned above. Care should be taken that seemingly duplicate records have not been annotated.

✓ Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the Authority's policies, relevant legislation and regulatory guidance.

✓ Where relevant to do so we will carry out a data privacy impact assessment and update our privacy notices to reflect data sharing.

Data Security:

✓ All employees are responsible for ensuring that: Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorized third party.

✓ Employees should note that unauthorized disclosure and/or failure to adhere to the requirements set out above will usually be a disciplinary matter, and may be considered gross misconduct in some Data cases.

✓ Personal information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerized, be password protected; or when kept or in transit on portable media the files themselves must be password protected.

✓ Personal data should never be stored at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

✓ Ordinarily, personal data should not be processed at employees' homes, whether in manual or electronic form, on

- ✓ laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller must be obtained, and all the security guidelines given in this document must still be followed.
- ✓ Data stored on portable electronic devices or removable media is the responsibility of the individual employee who operates the equipment.

An Audit Trail:

- ✓ You do not need to document the disposal of records which have been listed on the records retention schedule. Documents disposed out of the schedule either by being disposed of earlier or kept for longer than listed will need to be recorded for audit purposes.
- ✓ This will provide an audit trail for any inspections conducted by the regulatory and will aid in addressing Freedom of Information requests, where we no longer hold the material.

Monitoring:

- ✓ Responsibility for monitoring the disposal policy rests with the designated officer. The policy will be reviewed annually or more often as required.

Change in the Policy will be adopted as and when required by the company and is binding on all the Employees/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

LIMIT SETTING POLICY

Circular: - Ref.

Policy created by	Compliance Team
Policy reviewed by	Jitesh Dineshchandra Gandhi
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

Objective

To pre- define limits for each terminal and monitor the same on a continuous basis.

Background

Trading Terminals are allotted to Members by exchanges. These terminals enable members to place, modify and execute orders on behalf of clients. There may be instances where due to punching error unusual orders may be placed at high prices which might lead to execution of unrealistic orders or orders being executed at unrealistic prices. In cases where the order/price of such orders is high, it might lead to huge losses to broker. In order to avoid such a situation, it is imperative that certain limits are prescribed for each terminal allotted to member broker.

Scope of the Policy

This policy covers the procedure and checks and balances in place for allotting limits to each direct and CTCL / IML terminals.

Defining of Limits

The following limits shall be defined for each terminal:

- Quantity Limit for each order
- Value Limit for each order
- User value limit for each user ID
- User quantity limit for each user ID
- Branch value limit for each Branch ID
- Spread Order Quantity and Value Limit (Equity Derivatives segment)
- Market Price Protection Percentage

Procedure for setting of Limits

The company follows the practice of setting of limits at each level namely Admin, Branch Manager, Direct Terminal / CTCL / IML and Dealer. The limits have been set each level is reviewing the historical data of peak utilization at respective levels. Limits are reviewed on a regular basis and if required revised post consultation of Compliance Officer during the day. The Limits utilization is continuously monitored during the day. Any request of upward revision in limits by dealer is done post receipt of specific consent of Branch Head and after necessary risk assessment.

Checks in place

- Limits of terminals will be defined and reassigned on daily basis only after analyzing past trading history and assessment of risk.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

- Terminals limits will be set up by the Front Office official designated at Registered Office.
- No user/ branch will be provided unlimited limit.

Review of process and maintenance of records

The Compliance Officer at Registered Office shall be responsible for maintenance of records as prescribed by regulators and demonstrating the adequacy of system to auditors and exchanges.

The process of setting of limits shall be reviewed on a quarterly basis by Compliance officer and review the process on test check basis. The Compliance officer shall issue a certificate to the exchange on quarterly basis.

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 IDENTIFICATION OF CRITICAL ASSETS BASED ON SENSITIVITY

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 – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this Critical Asset Identification Policy is to establish guidelines and procedures for the identification and classification of critical assets based on sensitivity at [Your Company Name], a stock brokerage firm. This policy aims to ensure the prioritized protection and security of assets crucial to the firm's operations, compliance, and client trust.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals involved in the identification and classification of critical assets within the stock brokerage firm.

Policy Guidelines

Asset Identification Criteria

- Assets will be identified based on their significance to the firm's operations, regulatory compliance, and client services.
- Criteria for identification include financial impact, legal requirements, operational dependence, and potential harm in case of compromise.

Data Sensitivity Classification

- Data will be classified based on its sensitivity and importance to the business.
- Each classification level will determine the security controls and access restrictions for the identified critical assets.

Identification Process

- A systematic process will be established to identify critical assets, involving collaboration between business units, IT, security, and compliance teams.
- The identification process will be periodic and reactive to changes in the business environment.

Asset Inventory

- A comprehensive inventory of critical assets will be maintained, including but not limited to financial data, client information, trading platforms, and communication systems.
- The inventory will include details such as asset type, classification, owner, and associated risks.

Access Control

- Access to critical assets will be restricted based on their sensitivity classification.
- Access permissions will be regularly reviewed and adjusted as necessary.

Data Encryption

- Encryption will be applied to critical data assets, both in transit and at rest.
- Encryption protocols will align with industry standards and regulatory requirements.

Physical Security Measures

- Critical physical assets, such as servers and communication infrastructure, will be housed in secure locations with access controls and monitoring.
- Adequate measures will be taken to protect against physical threats.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Incident Response Plan for Critical Assets

- An incident response plan specifically addressing critical assets will be established to ensure a swift and effective response in case of security incidents.
- Regular testing and updates of the incident response plan will be conducted.

Compliance and Legal Considerations

Regulatory Compliance

- The asset identification and protection processes will comply with relevant financial regulations and industry standards.
- Regular audits will be conducted to verify compliance.

Review and Update

This policy will be reviewed regularly and updated as necessary to address changes in the business environment, regulatory requirements, and emerging security threats.

Employee Responsibilities

Employees involved in the identification and management of critical assets are responsible for adhering to this policy and promptly reporting any concerns or incidents.

Training and Awareness

- Employees will undergo training on critical asset identification, classification, and protection.
- Awareness campaigns will be conducted to foster a culture of responsibility and security.

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 DATA SECURITY

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 – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this Data Security Policy is to establish guidelines and procedures for protecting the confidentiality, integrity, and availability of data at our Company. This policy aims to mitigate the risk of unauthorized access, disclosure, alteration, and destruction of sensitive financial information.

Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have access to the stock brokerage firm's data and information systems.

Policy Guidelines

Data Classification

- Data will be classified based on its sensitivity and importance to the business.
- Each classification level will have corresponding security controls and access restrictions.

Access Control

- Access to sensitive data will be restricted based on job responsibilities and the principle of least privilege.
- User access will be reviewed regularly, and adjustments will be made as needed.

Data Encryption

- Encryption will be applied to sensitive data in transit and at rest.
- Encryption protocols will comply with industry standards.

Secure Transmission

- Secure communication protocols, such as HTTPS, will be used for transmitting sensitive data over networks.
- Public networks, including the internet, will be avoided for transmitting sensitive information.

Secure Storage

- Sensitive data will be stored securely in designated repositories with access controls.
- Physical and logical security measures will be implemented to protect data storage facilities.

Data Backup and Recovery

- Regular backups of critical data will be conducted to ensure data availability in the event of system failures or disasters.
- Backup and recovery procedures will be tested periodically.

Endpoint Security

- Endpoint security solutions, including antivirus software and endpoint detection and response (EDR) tools, will be deployed and regularly updated.
- Mobile devices used for work purposes will adhere to the same security standards.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Incident Response Plan

- An incident response plan will be established to promptly address and mitigate security incidents.
- Employees will be trained on reporting security incidents.

Vendor Security

- Third-party vendors with access to sensitive data will be evaluated for security controls and compliance with data security standards.
- Contracts with vendors will include data security requirements.

Compliance and Legal Considerations

Regulatory Compliance

- The data security policy will comply with relevant financial regulations and industry standards.
- Regular audits will be conducted to verify compliance.

Review and Update

This policy will be reviewed regularly and updated as necessary to address emerging security threats and technological advancements.

Employee Responsibilities

Employees are responsible for using data in accordance with this policy and reporting any suspicious activities promptly.

Confidentiality Agreement

Employees will sign a confidentiality agreement, acknowledging their responsibility for protecting sensitive data.

Training and Awareness

- Employees will undergo regular training on data security best practices.
- Awareness campaigns will be conducted to ensure a culture of security.

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.

JDGuJL

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

BRING YOUR OWN DEVICE POLICY

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 – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this Bring Your Own Device (BYOD) policy is to establish guidelines for the secure and productive use of personal devices by employees at our Company. This policy outlines the responsibilities of both employees and the organization to ensure the confidentiality, integrity, and availability of sensitive financial information.

Scope

This policy applies to all employees, contractors, and third-party vendors who use personal devices to access company resources, data, or systems.

Policy Guidelines

Eligibility

- Employees eligible for BYOD must meet certain security and compliance criteria determined by the IT department.

Device Security Requirements

- Devices must have up-to-date antivirus software and security patches.
- Employees must use strong, unique passwords or passcodes to access devices.
- Devices must be configured to automatically lock after a specified period of inactivity.

Data Protection

- Employees must adhere to data classification policies and take necessary precautions to protect sensitive financial data.
- Company data should not be stored on personal devices unless authorized by the IT department.

Network Security

- Employees must connect to secure and password-protected Wi-Fi networks.
- Public Wi-Fi networks should be avoided when accessing company resources.

Software and Application Management

- Only authorized software and applications should be installed on personal devices.
- Employees are responsible for keeping software and applications up to date.

Compliance and Legal Considerations

Regulatory Compliance

- All activities conducted on personal devices must comply with relevant financial regulations and industry standards.

Monitoring and Auditing

- The organization reserves the right to monitor and audit personal devices for security and compliance purposes.

Employee Responsibilities

- Employees are responsible for the security of their personal devices used for work purposes.

- Promptly report lost or stolen devices to the IT department.
- Report any suspicious activity or security incidents to the IT department.

Termination of Access

Access to company resources via personal devices may be revoked at any time, especially in the event of a security breach or termination of employment.

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

NETWORK SECURITY POLICY

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 – 1.0

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Purpose

The purpose of this Network Security Policy is to establish guidelines and procedures to secure the network infrastructure, data, and communication systems of our Company. This policy aims to mitigate risks, protect sensitive information, and ensure the availability and reliability of network resources.

Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to the stock brokerage firm's network infrastructure and systems.

Policy Guidelines

Access Control

- Access to the network and systems shall be granted based on job responsibilities.
- User accounts must be unique to individuals and tied to specific job roles.
- Access permissions will be reviewed regularly and adjusted as needed.

Authentication and Passwords

- Strong, unique passwords are required for all user accounts.
- Multi-factor authentication (MFA) is mandatory for accessing sensitive systems.
- Passwords must be changed at regular intervals.

Network Monitoring

- Network traffic will be monitored for abnormal patterns and potential security threats.
- Regular audits of network logs will be conducted to identify and respond to suspicious activities.

Firewall Configuration

- Firewalls must be configured to restrict unauthorized access and protect against external threats.
- Regular reviews of firewall rules and configurations will be conducted.

Data Encryption

- All sensitive data transmitted over the network must be encrypted using secure protocols.
- Virtual Private Network (VPN) connections are required for remote access.

Wireless Network Security

- Wireless networks must be secured with strong encryption and authentication mechanisms.
- Guest Wi-Fi networks should be isolated from the main network.

Incident Response Plan

- An incident response plan will be established to promptly address and mitigate security incidents.
- Employees shall be trained on reporting security incidents and breaches.

Remote Access Security

- Remote access to company networks must adhere to the same security standards as on-site access.
- Secure connections, such as VPNs, must be used for remote access.

CORUM SECURITIES PVT. LTD.

Authorised Signatory/Director

Vendor Security

Third-party vendors with network access must comply with security standards and undergo periodic security assessments.

Compliance and Legal Considerations

Regulatory Compliance

The network security policy will adhere to relevant financial regulations and industry standards.

Audit and Assessment

Periodic audits and security assessments will be conducted to ensure compliance with this policy.

Employee Responsibilities

Employees are responsible for using the network resources in a secure and responsible manner.

Any suspicious activity or potential security vulnerabilities must be reported promptly.

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