

# 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

### BACKUP 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 Backup Policy is to establish guidelines and procedures for the regular and secure backup of critical data at our Company. This policy aims to ensure the availability, integrity, and recoverability of data in the event of data loss, system failures, or unforeseen disasters.

## Scope

This policy applies to all employees, contractors, and third-party vendors who have access to and are responsible for managing critical data within the stock brokerage firm.

## Policy Guidelines

### **Data Classification**

- Data will be classified based on its sensitivity and importance to the business.
- Backup strategies will be aligned with the classification of data.

### **Backup Frequency**

- Critical data will be backed up regularly, with the frequency determined by the data's criticality and change rate.
- Full system backups will be performed periodically.

### **Backup Storage**

- Backup data will be stored in secure, offsite locations to protect against on-site disasters.
- Multiple copies of backup data will be maintained to ensure redundancy.

### **Retention Period**

- Backup retention periods will be established based on regulatory requirements, business needs, and data classification.
- Old backups will be periodically reviewed and purged in compliance with retention policies.

### **Encryption**

- Backup data, both in transit and at rest, will be encrypted using industry-standard encryption algorithms.
- Encryption keys will be securely managed.

### **Testing and Verification**

- Regular tests and verifications of backup and restore procedures will be conducted to ensure data recoverability.
- Testing will include both full and incremental backups.

### **Documentation**

- Comprehensive documentation of backup procedures, schedules, and restoration processes will be maintained.
- Employees responsible for backup procedures will be adequately trained.

### **Monitoring and Alerts**

- Backup systems will be monitored for any failures or anomalies.
- Alerts will be generated and promptly addressed to maintain the integrity of the backup process.

**CORUM SECURITIES PVT. LTD.**

# 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

## Compliance and Legal Considerations

### Regulatory Compliance

- The backup policy will adhere to relevant financial regulations and industry standards.
- Regular audits will be conducted to ensure compliance.

### Audit and Assessment

Periodic audits and assessments will be conducted to evaluate the effectiveness of the backup policy and procedures.

## Employee Responsibilities

Employees are responsible for adhering to backup procedures and promptly reporting any issues or concerns related to data protection.

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

### BCP AND RESPONSE MANAGEMENT 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 Business Continuity Planning (BCP) and Response Management Policy is to establish guidelines and procedures to ensure the continuity of critical business operations, mitigate the impact of disruptions, and provide a structured response to emergencies or unforeseen events at our Company.

## Scope

This policy applies to all employees, contractors, and third-party vendors who have responsibilities related to the business continuity and response management efforts of the stock brokerage firm.

## Policy Guidelines

### **Risk Assessment and Business Impact Analysis (BIA)**

- Regular risk assessments and BIAs will be conducted to identify potential threats and assess their impact on critical business functions.
- Findings from risk assessments and BIAs will inform the development and updating of the BCP.

### **Business Continuity Planning (BCP) Framework**

- A comprehensive BCP framework will be established to guide the development, implementation, and maintenance of business continuity plans.
- BCPs will address various scenarios, including but not limited to technology failures, natural disasters, and pandemics.

### **Emergency Response Plan**

- An Emergency Response Plan will be developed to provide clear guidelines for immediate response to emergencies.
- Roles and responsibilities during emergencies will be clearly defined.

### **Communication Protocols**

- Effective communication protocols will be established to ensure timely and accurate dissemination of information during emergencies.
- Communication channels will be diverse to accommodate various scenarios.

### **Employee Training and Awareness**

- Employees will receive regular training on their roles and responsibilities during emergencies.
- Awareness campaigns will be conducted to ensure all employees are familiar with the BCP and Emergency Response Plan.

### **Alternative Work Arrangements**

- Plans for alternative work arrangements, such as remote work, will be in place to ensure continuity in the event of office unavailability.
- Technology infrastructure will be equipped to support remote work.

### **Data and System Backup**

- Data backup and system recovery procedures will be established to ensure the availability of critical systems and data during disruptions.
- Regular testing of backup and recovery processes will be conducted.

**CORUM SECURITIES PVT. LTD.**

# 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

## Testing and Exercises

- Regular testing and simulation exercises will be conducted to assess the effectiveness of the BCP and response plans.
- Findings from exercises will inform updates and improvements to the plans.

## Coordination with External Partners

- Coordination with external partners, such as regulators and key vendors, will be established to ensure a collaborative and effective response during emergencies.

## Compliance and Legal Considerations

### Regulatory Compliance

- The BCP and response management efforts will comply with relevant financial regulations and industry standards.
- Periodic audits will be conducted to verify compliance.

### Review and Update

- This policy will be reviewed regularly and updated as necessary to address emerging risks, technological advancements, and regulatory changes.


## Employee Responsibilities

- Employees are responsible for familiarizing themselves with the BCP and Emergency Response Plan and following guidelines during emergencies.
- Reporting incidents promptly is crucial to effective response and recovery efforts.

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

### PASSWORD POLICY:

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 - 1.2

CORUM SECURITIES PVT. LTD.

  
Authorised Signatory/Director

### Purpose:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

### Scope:

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the NIC domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

### Policy:

#### Policy Statements

- ✓ For users having accounts for accessing systems/services
- ✓ Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.
- ✓ All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.
- ✓ Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
- ✓ Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
- ✓ All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.
- ✓ All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.
- ✓ Passwords must not be communicated through email messages or other forms of electronic communication such as phone to anyone.
- ✓ Passwords shall not be revealed on questionnaires or security forms.
- ✓ Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.
- ✓ The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected.
- ✓ The "Remember Password" feature of applications shall not be used.
- ✓ Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.
- ✓ First time login to systems/services with administrator created passwords, should force changing of password by the user.
- ✓ If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.



The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

- ✓ For designers/developers of applications/sites
- ✓ No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.
- ✓ The backend database shall store hash of the individual passwords and never passwords in readable form.
- ✓ Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
- ✓ Users shall be required to change their passwords periodically and not be able to reuse previous passwords.
- ✓ For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

### **Policy for constructing a password:**

All user-level and system-level passwords must conform to the following general guidelines described below.

- ✓ The password shall contain more than eight characters.
- ✓ The password shall not be a word found in a dictionary(English or foreign).
- ✓ The password shall not be a derivative of the user ID, e.g. <username>123.
- ✓ The password shall not be a slang, dialect, jargon etc.
- ✓ The password shall not be a common usage words such as names of family, pets, friends, co-workers, fantasy characters, etc.
- ✓ The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.
- ✓ The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
- ✓ The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.
- ✓ The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- ✓ The password shall be a combination of upper- and lower-case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., @# \$%^&\*() \_+ | ~- = \ ` { } [] : ; ' < > ? / ).
- ✓ Passwords shall not be such that they combine a set of characters that do not change with a set of charactersthat predictably change.

### **Suggestions for choosing passwords:**

- ✓ Passwords may be chosen such that they are difficult-to-guess yet easy-to- remember. Methods such as the following may be employed:
- ✓ String together several words to form a pass-phrase as a password.
- ✓ Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.
- ✓ Combine punctuation and/or numbers with a regularword.
- ✓ Create acronyms from words in a song, a poem, or anyother known sequence of words.

**CORUM SECURITIES PVT. LTD.**

# 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

- ✓ Bump characters in a word a certain number of letters up or down the alphabet
- ✓ Shift a word up, down, left or right one row on the keyboard.

## Responsibilities:

- ✓ All individual users having accounts for accessing systems/services in the NIC domain, and system/network administrators of NIC servers' / network equipment shall ensure the implementation of this policy.
- ✓ All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

## Compliance

- ✓ Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.
- ✓ Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

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.**

*J D Gandhi*  
\_\_\_\_\_  
**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

### LOG 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 - 1.0

CORUM SECURITIES PVT. LTD.

*J D Kundu*  
Authorised Signatory/Director

## Purpose

The purpose of this Log Retention Policy is to establish guidelines and procedures for the retention, management, and secure disposal of logs at our Company. This policy aims to ensure the availability of logs for operational needs, compliance with regulations, and effective response to security incidents.

## Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who have access to or are responsible for managing logs within the stock brokerage firm.

## Definitions

### **Logs**

Records generated by systems, applications, networks, and security devices that capture events, transactions, or interactions.

### **Log Retention**

The period for which logs are stored and maintained.

## Policy Guidelines

### **Identification of Critical Logs**

Critical logs, including but not limited to security event logs, system logs, and application logs, will be identified based on their significance to operations, compliance, and security.

### **Retention Periods**

- Retention periods for logs will be determined based on regulatory requirements, legal obligations, and business needs.
- Different types of logs may have different retention periods.

### **Log Storage**

- Logs will be stored in a secure, centralized repository with restricted access.
- Adequate measures will be taken to protect log storage facilities physically and logically.

### **Encryption of Stored Logs**

Logs stored for an extended period will be encrypted to ensure the confidentiality and integrity of the information.

### **Regular Review of Logs**

- Logs will be regularly reviewed to identify anomalies, security incidents, and operational issues.
- Automated tools may be used to assist in log analysis.

**CORUM SECURITIES PVT. LTD.**

# 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

## Disposal of Obsolete Logs

Logs that have exceeded their retention period or are no longer relevant will be securely disposed of using industry-accepted methods.

## Legal Hold

In case of legal proceedings or investigations, a legal hold may be applied to prevent the disposal of relevant logs.

## Monitoring and Auditing

The log retention process will be monitored, and periodic audits will be conducted to ensure compliance with this policy.

## Compliance and Legal Considerations

### Regulatory Compliance

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

### Documentation

Detailed records of log retention periods, disposal processes, and audit results 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

### IT ACCESS CONTROL AND USER ACCESS MANAGEMENT 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.

*J.D. Ghosh*  
Authorised Signatory/Director

## Policy Statement

- Protecting access to IT systems and applications is critical to maintain the integrity of the Company's technology and data and prevent unauthorized access to such resources.
- Access to Company's systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

## Background

- Access controls are necessary to ensure only authorized users can obtain access to the Company's information and systems.
- Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job-related duties.

## Policy Objective

- The objective of this policy is to ensure the Institution has adequate controls to restrict access to systems and data.

## Scope

- This policy applies to all branch and head office including employees, Consultants and Outside Vendors accessing Company's IT systems and applications.

## Definitions

- "Access Control" is the process that limits and controls access to resources of a computer system.
- "Users" are employees, consultants, contractors, agents and authorized users accessing Company IT systems and applications.
- "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.
- "Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.
- "Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.
- "Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.
- "Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.
- "Nominative User Accounts" are user accounts that are named after a person.
- "Non-disclosure Agreement" is a contract between a person and the Company stating that the person will protect confidential information (as defined in the Record Classification and Handling Policy) covered by the contract, when this person has been exposed to such information.

### Guiding Principles - General Requirements

- The Company will provide access privileges to Company technology (including networks, systems, applications, computers and mobile devices) based on the following principles:
  - **Need to know** - users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
  - **Least privilege** - users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.
- Requests for users' accounts and access privileges must be formally documented and appropriately approved.
- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the system owner.
- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.
- Where possible, the Company will set user accounts to automatically expire at a pre-set date. More specifically,
  - When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
  - User accounts assigned to contractors will be set to expire according to the contract's expiry date.
  - User accounts will be disabled after 3 months of inactivity. This does not apply to accounts assigned to employees.
  - User accounts with signed contracts for a recurring, continuing, or tenure track appointment for an upcoming term can be active for up to four months between appointments.
- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access Company's systems.
- A verification of the user's identity must be performed by the IT Director, Help Desk, or designate before granting a new password.
- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:
  - An active account assigned to external contractors, vendors or employees that no longer work for the Company.
  - An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
  - System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.
  - Unknown active accounts.
- All access requests for system and application accounts and permissions will be documented using the ticketing system in place.

CORUM SECURITIES PVT. LTD.



### Guiding Principles - Privileged Accounts

- A nominative and individual privileged user account must be created for administrator accounts (such as "first name. last name. admin"), instead of generic administrator account names.
- Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.

### Guiding Principles - Shared User Accounts

- Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts.
- Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional" accounts.
- When shared accounts are required:
  - Passwords will be stored and handled in accordance with the Password Policy.
  - The use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his account. When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected and restricted.

### Vendor or Default User Accounts

- Where possible, all default user accounts will be disabled or changed. These accounts include "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off-the-shelf" systems and applications.

### Test Accounts

- Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the IT Director or the IT Help Desk.
- Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.
- Test accounts will be disabled / deleted when they are no longer necessary.

### Contractors and Vendors

- In accordance with the Contract Management Policy, contracts with contractors / vendors will include specific requirements for the protection of data. In addition, contractor / vendor representatives will be required to sign a Non-disclosure Agreement ("NDA") prior to obtaining approval to access Institution systems and applications.
  - Prior to granting access rights to a contractor / vendor, the IT Director or Help Desk must verify the requirements of Section 11.1 have been complied with.
  - The name of the contractor / vendor representative must be communicated to the IT Help Desk at least 2 business days before the person needs access.
- The Company will maintain a current list of external contractors or vendors having access to Company's systems.
- The need to terminate the access privileges of the contractor / vendor must be communicated to the IT Help Desk at

least 1 business day before the contractor / vendor representative's need for such access ends.

### Access Control Requirements

- All users must use a unique ID to access Company's systems and applications. Passwords must be set in accordance with the Password Policy.
- Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.
  - Remote access to Company's systems and applications must use two-factor authentication where possible.
  - System and application sessions must automatically lock after 15 minutes of inactivity.

### Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Board of Director	<ul style="list-style-type: none"> <li>• Approve and formally support this policy.</li> </ul>
President, Administration	<ul style="list-style-type: none"> <li>• Review and formally support this policy.</li> </ul>
IT Director/Designated officer	<ul style="list-style-type: none"> <li>• Develop and maintain this policy.</li> <li>• Review and approve any exceptions to the requirements of this policy.</li> <li>• Take proactive steps to reinforce compliance of all stakeholders with this policy.</li> </ul>
Supervisors or Company's Representative	<ul style="list-style-type: none"> <li>• Support all employees and others in the understanding of the requirements of this policy.</li> <li>• Immediately assess and report to the IT service desk any non-compliance instance with this policy.</li> </ul>
Contract Administrators	<ul style="list-style-type: none"> <li>• Ensure that the responsibilities and security obligations of each party to the contractual relationship are outlined in the contract executed between the Company's and the contractor/sub-contractor.</li> </ul>
Human Resources	<ul style="list-style-type: none"> <li>• Present each new employee or contractor with the relevant Company's IT and Security Policies, upon the first day of commencing work with Company's.</li> <li>• Support all employees and other in the understanding of the requirements of this policy.</li> </ul>
All users (Employees and contractors, Visitors and or Volunteers)	<ul style="list-style-type: none"> <li>• Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Company's Representative as soon as possible.</li> </ul>

### Exceptions to the Policy

- Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director/Designated Officer.
- **Policy exceptions must describe:**
  - The nature of the exception
  - A reasonable explanation for why the policy exception is required

CORUM SECURITIES PVT. LTD.

*J. D. S.*  
Authorised Signatory/Director

# 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

- Any risks created by the policy exception
- Evidence of approval by the IT Director
- **Inquiries**
  - Inquiries regarding this policy can be directed to the IT Director/Designated officer.

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.**

*J D Gandhi*

**Authorised Signatory/Director**

(Jitesh Dineshchandra Gandhi)

Designated Director

Dated: - 02/01/2024

CONFIDENTIAL

# 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

### INTERNET ACCESS 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.

*J D Guha*  
Authorised Signatory/Director

## Objective

Our organisation recognizes that use of the Internet and e-mail is necessary in the workplace, and employees are encouraged to use the Internet and e-mail systems responsibly, as unacceptable use can place Company and others at risk. This policy outlines the guidelines for acceptable use of Company's technology systems. This policy helps ensure network security, protect sensitive information, and promote responsible and productive use of internet resources.

## Scope

This policy must be followed in conjunction with other policies governing appropriate workplace conduct and behaviour. Any employee who abuses the company-provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access and, if appropriate, be subject to disciplinary action up to and including termination. Company complies with all applicable central, state and local laws as they concern the employer/employee relationship, and nothing contained herein should be misconstrued to violate any of the rights or responsibilities contained in such laws.

Questions regarding the appropriate use of Company's electronic communications equipment or systems, including e-mail and the Internet, should be directed to your supervisor or the information technology (IT) department.

## Policy

Company has established the following guidelines for employee use of the company's technology and communications networks, including the Internet and e-mail, in an appropriate, ethical and professional manner.

### **Confidentiality and Monitoring**

- All technology provided by Company, including computer systems, communication networks, company-related work records and other information stored electronically, is the property of the Company and not the employee. In general, use of the company's technology systems and electronic communications should be job-related and not for personal convenience. Company reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite.
- Internal and external e-mail, voice mail, text messages and other electronic communications are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company.

### **Appropriate Use**

- Company employees are expected to use technology responsibly and productively as necessary for their jobs. Internet access and e-mail use is for job-related activities; however, minimal personal use is acceptable.
- Employees may not use Company's Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.
- Disparaging, abusive, profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail—are forbidden.

**CORUM SECURITIES PVT. LTD.**

# 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

- Copyrighted materials belonging to entities other than Company may not be transmitted by employees on the company's network without permission of the copyright holder.
- Employees may not use Company's computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and spamming (sending unsolicited e-mail to thousands of users).
- Employees are prohibited from downloading software or other program files or online services from the Internet without prior approval from the IT department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into company systems and networks.
- Every employee of Company is responsible for the content of all text, audio, video or image files that he or she places or sends over the company's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Company's corporate identity is attached to all outgoing e-mail communications, which should reflect corporate values and appropriate workplace language and conduct.
- Every employee should emphasize the importance of maintaining strong and secure passwords for internet access and encourage regular password updates and provide guidelines for creating strong passwords.

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.



Authorized 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

### TECHNICAL GLITCHES POLICY

Circular: - Ref. SEBI/HO/MIRSD/TPD-1/P/CIR/2022/160 dated November 25, 2022

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.

J D G  
Authorised Signatory/Director

## Objective

o establish a comprehensive framework for addressing and mitigating technical glitches in electronic trading systems, ensuring investor protection and market integrity.

## Definition of Technical Glitch

A technical glitch refers to any malfunction in the stock broker's systems, including hardware, software, networks, processes, or services provided electronically. This malfunction may lead to stoppage, slowing down, or variance in normal system functions for a contiguous period of five minutes or more.

## Reporting Requirements

- We will inform the respective stock exchanges about any technical glitch, not later than one hour from the time of occurrence.
- Submission of a Preliminary Incident Report to the Exchange within T+1 day of the incident, including details of the incident, its impact, and immediate actions taken.
- Submission of a Root Cause Analysis (RCA) Report to the stock exchange within 14 days, covering the incident's cause, duration, impact analysis, and corrective/preventive measures. The RCA report, for all technical glitch incidents greater than 45 minutes, an independent auditor's report on the RCA shall be submitted within 45 days of the incident.

## Capacity Planning

- We will conduct regular capacity planning for their trading infrastructure, including servers, network availability, and trading applications.
- Monitoring peak load with installed capacity at least 1.5 times the observed peak load.
- Deploying mechanisms to receive alerts on capacity utilization beyond 70% of installed capacity.

## Software Testing and Change Management

- Rigorous testing of all software changes before deployment.
- Creation of test-driven environments, automated testing, and a traceability matrix between functionalities and unit tests.
- Implementation of a change management process to prevent unplanned and unauthorized changes.

## Monitoring Mechanism

- Establishment of an API-based Logging and Monitoring Mechanism (LAMA) between stock exchanges and stock brokers' trading systems.
- Real-time or near-real-time monitoring of key parameters by both stock brokers and stock exchanges.
- We ensure to preserve the logs of the key parameters for a period of 30 days in normal course. However, if a technical glitch takes place, the data related to the glitch, shall be maintained for a period of 2 years.



# 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

## Business Continuity Planning (BCP) and Disaster Recovery Site (DRS)

- Mandatory establishment of BCP-DR set up for stock brokers with a specified client base i.e. 'Specified Members'.
- Periodic review of BCP-DR policy outlining standard operating procedures.
- Conducting DR drills/live trading from DR site, ensuring full redundancy and ISO certification.

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