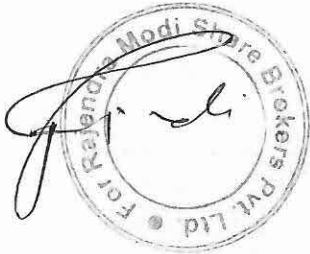




**Rajendra Modi Share
Brokers Private Limited**
Members of NSE, BSE, CDSL, MCX

Name of the Policy	ACCESS CONTROL POLICY
Date of Passing Board Resolution	7 th April, 2026
Approved by:	Board of Directors
Frequency of Review:	Yearly or as and when any update comes change in the Relevant Regulation comes or any change in the Company's internal control or Structure whichever is earlier.



For Rajendra Modi Share Brokers Pvt. Ltd.

[Signature]
Managing Director



403-404, 508, Green House,
Ashok Marg, C-Scheme, Jaipur-302001



CIN : U67120RJ2007PTC023636



rajndrmodi@yahoo.com / rajendra@rmsbplindia.com / khushi@rmsbplindia.com



2369004-5, 2369006-7



0141-5115775



www.rmsbplindia.com

ACCESS CONTROL POLICY

Purpose

The purpose of this policy is to ensure that access to the Company's information systems, applications, networks, and data is granted only to authorized users based on business requirements and security needs.

Scope

This policy applies to all employees, directors, consultants, contractors, vendors, business partners, and any other individuals who have access to the Company's information assets, systems, applications, and networks.

Policy Statement

Access to information systems and business applications shall be granted strictly on a need-to-know and need-to-use basis. Users shall only be provided access necessary to perform their assigned job responsibilities.

User Access Management

User Registration and De-registration

- Every user shall be assigned a unique User ID/Client ID.
- Access shall be provided only after proper authorization from the concerned department or system owner.
- User access rights shall be documented and maintained.
- User accounts of employees leaving the organization shall be disabled immediately.
- User accounts shall be reviewed periodically to identify inactive, redundant, or unauthorized access.
- User accounts password gets automatic expiry at the end of a reasonable duration (maximum 90 Days) and re-initialization of access on entering fresh passwords.



Privileged Access

- Administrative and privileged access rights shall be granted only through formal approval.
- Privileges shall be assigned on the principle of least privilege and only when required for business purposes.
- Privileged accounts shall be reviewed periodically.

Password Management

- All users shall comply with the Company's Password Policy.
- Temporary passwords must be changed at first login.
- Passwords shall not be shared, written down, or stored in publicly accessible locations.
- Passwords of administrators or employees leaving the organization shall be changed immediately where applicable.
- Forgotten passwords shall be reset only after proper user verification.

Access Review

- User access rights shall be reviewed at least once every six months.
- Privileged access rights shall be reviewed at least once every three months.

User Responsibilities

- Users shall maintain the confidentiality of their login credentials.
- Systems shall be protected using password-protected screen locks.
- Screen locks shall activate after a maximum of 15 minutes of inactivity.
- Users shall log off or lock systems when not in use.

Network Access Control

- Access to network resources shall be provided only after authorization.
- Internal and external networks shall be segregated using appropriate security controls.
- External connections shall be approved, documented, and monitored.
- Network traffic shall be controlled through firewalls and routing controls.



System Access Control

- All users shall be uniquely identified and authenticated before accessing systems.
- User IDs shall not be shared.
- Access to system utilities and administrative tools shall be restricted to authorized personnel only.
- User sessions shall be automatically locked after a defined period of inactivity.
- Systems shall display appropriate security and legal warning banners before login.

Login Security Controls

- User accounts shall be locked after five consecutive unsuccessful login attempts.
- Login procedures shall not disclose whether the User ID or password was incorrect.
- Users shall be informed of their previous successful login and unsuccessful login attempts.
- Authentication processes shall be designed to prevent unauthorized access.

Application and Information Access Control

- Access to applications and information shall be based on job roles and business requirements.
- Information owners shall review user access rights periodically.
- Sensitive systems and critical applications shall be hosted in secure and controlled environments.

Monitoring and Logging

- System activities and access logs shall be maintained and monitored.
- Logs shall be retained for at least three years and for longer periods where required by business or regulatory requirements.
- Unsuccessful login attempts and suspicious activities shall be investigated and escalated appropriately.
- System clocks shall be synchronized to ensure accurate logging and monitoring.



Shared Folders and Data Sharing

- Access to shared folders shall be restricted to authorized users only.
- Shared folders shall be used strictly for official business purposes.

Compliance

Compliance with this policy is mandatory. Violations may result in disciplinary action, including suspension or removal of system access privileges and other actions deemed appropriate by management.

Classification/Information

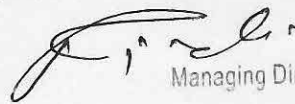
In case of any clarification/information required on the implementation of the Policy, please contact the IT Head/Compliance Officer on Email -rjndrmodi@yahoo.com

Review

The said policy shall be reviewed by the Board of the Directors on a yearly basis or as and when any update comes change in the Relevant Regulation/Circular comes or any change in the internal control or Structure. The Compliance officer has the authority to give direction to undertake additions, changes, and modifications, etc. to this Policy, and the same shall be effective per the authority of the Compliance Officer and thereafter be ratified by the Board of the Directors at its next review. Periodic audits will be conducted to ensure compliance with this policy



For Rajendra Modi Share Brokers Pvt. Ltd.


Managing Director