

BMD SECURITIES LIMITED

REMOTE ACCESS POLICY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2024
Policy Approved by	Board of Directors
Policy approved on	28-04-2025

Version - 1.0

BMD SECURITIES LIMITED

REMOTE ACCESS POLICY

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31-12-2023
Policy Approved by	Board of Directors
Policy approved on	28-01-2025

Version - 1.0

Purpose and Scope

This Remote Access Policy outlines the guidelines and procedures for remote access to our company's systems and data. The objective is to ensure secure and compliant remote access while safeguarding sensitive information and maintaining the integrity of our trading platform.

Authorized Remote Access

Eligibility

- Remote access is limited to authorized employees, contractors, and partners whose roles require it for business purposes.
- Approval for remote access will be granted based on job responsibilities and security considerations.

Approval Process

- Users must submit a remote access request, detailing the need for access and the duration.
- Approval will be granted by the IT Department after a review of the request.

Security Measures

Multi-Factor Authentication (MFA)

- Remote access requires the use of multi-factor authentication to enhance security.
- Users must configure and use approved MFA methods.

Secure Connection

- Remote access must be established through secure and encrypted channels (e.g., VPN or other approved methods) to protect data in transit.

Device Security

- Devices used for remote access must comply with the organization's security policies, including up-to-date antivirus software and operating system patches.

Data Protection and Confidentiality

- Users accessing company systems remotely must adhere to data protection and confidentiality policies.
- Sensitive information should not be stored locally on remote devices.

Logging and Monitoring

- Remote access activities will be logged and monitored for security and compliance purposes.

- Any suspicious or unauthorized activity will be investigated promptly.

Termination of Access

- Remote access will be revoked immediately upon the termination of employment or when access is no longer required for business purposes.

Compliance with Regulatory Requirements

- Remote access practices must adhere to all relevant regulatory requirements in the financial industry.
- Periodic reviews will be conducted to ensure ongoing compliance.

User Training and Awareness

- Users with remote access privileges will undergo training on security best practices and the organization's remote access policies.
- Regular awareness campaigns will be conducted to reinforce security protocols.

Reporting Security Incidents

- Users must report any suspected security incidents or unauthorized access immediately to the IT Department.

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.

BMD Securities Limited



Utpal Mallick

CISO

Dated: - 30-04-2025