ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

REMOTE ACCESS POLICY FOR STOCK BROKER & DEPOSITORY PARTICIPANTS

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

1. Introduction

This Remote Access Policy outlines the guidelines and procedures for granting and managing remote access to systems and resources for Stock Brokers and Depository Participants, with a strong focus on cybersecurity and resilience. This policy aims to ensure the security, confidentiality, integrity, and availability of information assets while enabling authorized remote access for authorized personnel, in compliance with the directives and circulars issued by the Securities and Exchange Board of India (SEBI).

2. Scope

This policy applies to all employees, contractors, and third-party vendors who require remote access to the systems and resources of the Stock Broker and Depository Participants. It covers all devices, networks, and applications used for remote access.

3. Policy Guidelines

3.1 Authorization

3.1.1 Remote access shall be granted only to authorized personnel who have a legitimate business need and have been vetted and approved by the designated authority.

3.1.2 Access privileges shall be assigned based on the principle of least privilege, ensuring that individuals are granted access to only the systems and resources necessary to perform their job functions.

- Authorization Procedure
- Authorized personnel requiring remote access shall submit a request to the designated authority, specifying the business need and the systems/resources they require access to.
- The designated authority shall review the request and verify the legitimacy of the business need. The authority will grant or deny access based on the principle of least privilege and in compliance with the Remote Access Policy.
- Upon approval, the designated authority shall assign the necessary access privileges to the authorized personnel, ensuring they have access only to the required systems and resources.

3.2 Multi-Factor Authentication (MFA)

3.2.1 Remote access shall be protected using multi-factor authentication mechanisms, such as a combination of passwords, one-time passwords (OTP), biometrics, or smart cards, as mandated by SEBI circulars and best practices.

3.2.2 MFA credentials shall be protected and securely stored, and individuals shall be educated about the importance of maintaining the confidentiality of their MFA tokens or devices.

- Multi-Factor Authentication (MFA) Procedure
- Authorized personnel shall be provided with MFA tokens, devices, or credentials, based on the organization's approved MFA mechanisms.
- Personnel shall be responsible for safeguarding their MFA tokens or devices and not sharing them with unauthorized individuals.
- MFA credentials shall be periodically updated, and personnel shall follow the organization's guidelines for secure management of their MFA tokens or devices.

3.3 Secure Connectivity

3.3.1 Remote access shall be established through secure channels, utilizing encrypted protocols such as Secure Socket Layer (SSL), Virtual Private Network (VPN), or other approved secure remote access technologies.

3.3.2 Remote access connections shall be configured to use strong encryption algorithms and periodically reviewed and updated as per the organization's security standards.

3.3.3 Network traffic monitoring and intrusion detection/prevention systems shall be implemented to detect and prevent unauthorized access attempts or suspicious activities.

- Secure Connectivity Procedure
- Authorized personnel shall establish remote access connections through approved secure channels, such as SSL, VPN, or other authorized remote access technologies.
- Personnel shall ensure that their remote access devices are configured to use strong encryption algorithms and comply with the organization's security standards.
- Before connecting to the remote access infrastructure, personnel shall verify the authenticity and validity of the SSL certificate or VPN server to mitigate the risk of man-in-the-middle attacks.

3.4 Endpoint Security

3.4.1 All remote access devices, including laptops, desktops, and mobile devices, shall comply with the organization's endpoint security standards, including the installation of approved anti-virus software, firewalls, and security patches.

3.4.2 Employees shall be responsible for regularly updating their remote access devices with the latest security patches and software updates.

3.4.3 Mobile devices used for remote access shall be protected with strong authentication, remote wipe capabilities, and encryption of sensitive data.

- Endpoint Security Procedure
- Personnel shall ensure that their remote access devices comply with the organization's endpoint security standards, including the installation of approved anti-virus software, firewalls, and security patches.
- Regular updates for operating systems and applications shall be applied promptly to address known vulnerabilities and protect against emerging threats.
- Mobile devices used for remote access shall have security measures in place, such as strong authentication, remote wipe capabilities, and encryption of sensitive data.

3.5 Session Monitoring and Logging

3.5.1 All remote access sessions shall be logged and monitored for security and compliance purposes.

3.5.2 Logs shall be stored securely, and access to logs shall be restricted to authorized personnel only.

3.5.3 Real-time monitoring tools shall be deployed to detect and alert on any suspicious activities or anomalies during remote access sessions.

- Session Monitoring and Logging Procedure
- Remote access sessions shall be logged and monitored for security and compliance purposes.
- The organization shall deploy monitoring tools to track and analyze remote access session activities, detect any suspicious behavior or unauthorized access attempts, and generate alerts for immediate response.
- Authorized personnel shall adhere to the organization's guidelines and restrictions regarding session monitoring and logging, understanding that their activities may be subject to review.

3.6 Data Protection and Confidentiality

3.6.1 Data transmitted and accessed during remote sessions shall be encrypted to protect its confidentiality and integrity.

3.6.2 Strong data access controls shall be implemented to prevent unauthorized data copying, downloading, or sharing during remote sessions.

3.6.3 Data classification and labeling mechanisms shall be established to ensure that sensitive data is appropriately protected during remote access.

- Data Protection and Confidentiality Procedure
- Authorized personnel shall ensure that data transmitted and accessed during remote sessions are encrypted using approved encryption protocols.
- Personnel shall comply with data protection guidelines, including refraining from unauthorized data copying, downloading, or sharing during remote access sessions.
- Sensitive data accessed remotely shall be classified and labeled appropriately to enforce necessary controls and ensure confidentiality.

3.7 Incident Reporting and Response

3.7.1 Any suspected or confirmed security incidents or breaches related to remote access shall be reported immediately to the designated authority.

3.7.2 The organization shall have an incident response plan in place, outlining the steps to be followed in the event of a security incident or breach.

3.7.3 Regular vulnerability assessments and penetration testing shall be conducted to identify and address potential security vulnerabilities in the remote access infrastructure.

- ➤ Incident Reporting and Response Procedure
- ➤ Any suspected or confirmed security incidents or breaches related to remote access shall be immediately reported to the designated authority or the organization's incident response team.
- ➤ Authorized personnel who notice any abnormal or suspicious activities during remote access sessions shall report them promptly.
- ➤ The incident response team shall follow the organization's established incident response plan to investigate, mitigate, and recover from security incidents or breaches.

4. Compliance

4.1 This policy shall comply with all applicable laws, regulations, and SEBI circulars related to remote access, cybersecurity, and resilience.

4.2 Regular audits and reviews shall be conducted to ensure compliance with this policy, and necessary updates and improvements shall be implemented as required.

4.3 Employees and authorized personnel shall be required to acknowledge their understanding and compliance with this policy on an annual or periodic basis.

- ➤ Compliance Monitoring Procedure
- ➤ Regular audits and reviews shall be conducted to assess compliance with the Remote Access Policy and associated procedures.
- ➤ Vulnerability assessments and penetration testing shall be performed periodically to identify and address any security vulnerabilities in the remote access infrastructure.
- ➤ Non-compliance or security issues identified during audits or assessments shall be documented, reported, and addressed through appropriate corrective actions.

Forms & Formats are annexed to this policy.

5. Policy Review

This policy has been reviewed, approved, and authorized by the designated authority of the Stock Broker and Depository Participants. This policy shall be communicated to all relevant employees, contractors, and third-party vendors. It shall be readily accessible in the organization's policy repository and included in employee training and awareness programs.

This policy shall be reviewed and updated as necessary to ensure its continued effectiveness and compliance with SEBI circulars, cybersecurity best practices, and any changes in the regulatory environment.

ANNEXURE TO POLICY

FORMS & FORMATS

1. Request for Remote Access Authorization

Date: [Date]
Employee/Contractor/Third-party Vendor Name: [Name]
Department/Team: [Department/Team]
Business Need for Remote Access: [Description of Business Need]
Systems/Resources Required: [List of Systems/Resources]
[Through registered email]

2. Approval:

Authorized Personnel/Designated Authority: [Name]
Date: [Date]
Access Privileges Granted:
System/Resource 1: [Access Level]
System/Resource 2: [Access Level]
...

Note: Please ensure that access privileges are based on the principle of least privilege, granting only the necessary access to perform job functions.

3. Remote Access Security Incident Report

Date and Time of Incident: [Date and Time]
Incident Details:
Description of Incident: [Description of the incident]
Affected Systems/Resources: [List of affected systems/resources]
Person(s) Involved: [Name(s) of personnel involved, if known]

Actions Taken:

Immediate Response and Mitigation Measures: [Description of immediate response and mitigation actions taken]
Investigation Findings: [Summary of investigation findings]
Root Cause Analysis: [Identification of the root cause of the incident, if determined]
Corrective Actions: [Description of corrective actions taken or recommended to prevent future incidents]
Reporting Person/Team:
Name: [Name]
Position/Department: [Position/Department]
Contact Information: [Email/Phone]

Note: This incident report should be submitted to the designated authority or incident response team as soon as the incident is detected or suspected.