

BYOD (Bring Your Own Device) Policy

Version	2023/02.01
Review Date	22/03/2024
Review & Approved by	Reviewed by Technology Committee & Approved by Board of Directors

1. Purpose:

The purpose of this BYOD policy is to establish guidelines and procedures to ensure the secure and productive use of personal devices by employees of the organization registered as a Stock Broker and Depository Participant. This policy aims to protect sensitive financial data, maintain regulatory compliance, and mitigate security risks associated with the use of personal devices for work-related activities.

2. Eligible Devices:

- Only smartphones, tablets, and laptops meeting the minimum security and compatibility requirements are eligible for BYOD.
- Eligible devices must have a supported operating system and receive regular security updates from the manufacturer.
- Employees must register their devices with the IT department for compliance and security purposes.

3. Security Software Requirements:

- All BYOD devices must have up-to-date antivirus and antimalware software installed.
- Employees must keep their security software enabled and regularly updated.
- IT department may periodically audit devices to ensure compliance with security software requirements.

4. Business-Grade VPN Service:

For, Genuine Stock Brokers Pvt. Ltd.



Manager / Director

Compliance Officer : Mr. Nikhil Agrawal, Email : genuine1996@gmail.com
 Regd./ Corporate Office : B-601, 6th Floor, Gopal Palace, Opp. Choice Restaurant, Nehru Nagar, Satellite Road,
 Ahmedabad - 380015. Ph. No : 079-40308992
 Member of NSE (10477) INZ000243831 BSE (3184) INZ000243831
 CIN No. U67120GJ1996PTC119507

- a. All BYOD devices must use a business-grade Virtual Private Network (VPN) service provided by the organization when accessing corporate networks or sensitive data remotely.
- b. Employees must connect to the VPN before accessing any corporate resources or confidential data.

5. Password and Authentication:

- a. Employees must set strong, unique passwords for their devices, using a combination of alphanumeric characters and special symbols.
- b. Devices should be configured to enforce password complexity and expiration policies.
- c. Employees should enable biometric authentication (e.g., fingerprint or facial recognition) where available and supported.

6. Data Encryption:

- a. Employees must enable device-level encryption on their BYOD devices to protect stored data.
- b. Encourage the use of encrypted communication channels (e.g., secure email and messaging apps) when transmitting sensitive information.

7. Device Management:

- a. The organization reserves the right to remotely manage and enforce security policies on registered BYOD devices, including updates, patches, and configurations.
- b. IT department may remotely wipe corporate data from a lost, stolen, or compromised device.

8. Acceptable Use:

- a. Employees should only access and store work-related information on their BYOD devices. Personal use should be limited during work hours.
- b. Prohibit the installation of unauthorized applications, games, or software on BYOD devices.
- c. Employees must not share corporate data or credentials with unauthorized individuals.

9. Incident Reporting:



- a. Employees must report any loss, theft, or suspected unauthorized access to their BYOD devices immediately to the IT department.
- b. Employees should promptly report any suspicious activities, security incidents, or policy violations related to their BYOD devices.

10. Compliance with Data Protection Regulations:

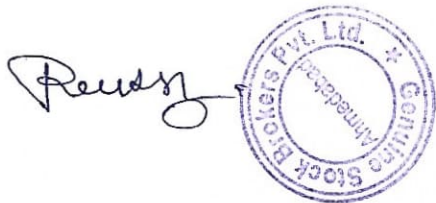
- a. All employees must adhere to applicable data protection and privacy regulations, including but not limited to the Securities and Exchange Board of India (SEBI) regulations.
- b. Personal and sensitive data must be handled in compliance with organizational policies and regulatory requirements.

11. Employee Training and Awareness:

- a. All employees must undergo regular training on BYOD policies, security best practices, and data protection regulations.
- b. Periodic awareness programs should be conducted to keep employees informed about emerging threats and security updates.

12. Policy Review:

- a. This BYOD policy will be reviewed periodically by the IT department to ensure its effectiveness and alignment with industry best practices and regulatory changes.
- b. Any updates or revisions to the policy will be communicated to all employees and documented accordingly.

The image shows a handwritten signature in blue ink, which appears to be "Remya", followed by a circular blue ink stamp. The stamp contains the text "Remya Stock Brokers Pvt. Ltd." around the perimeter and "Incorporated in India" in the center.