BMD SECURITIES LIMITED

BRING YOUR OWN DEVICE 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

Purpose

The purpose of this Bring Your Own Device (BYOD) policy is to establish guidelines for the secure and productive use of personal devices by employees at our Company. This policy outlines the responsibilities of both employees and the organization to ensure the confidentiality, integrity, and availability of sensitive financial information.

Scope

This policy applies to all employees, contractors, and third-party vendors who use personal devices to access company resources, data, or systems.

Policy Guidelines

Eligibility

- Employees eligible for BYOD must meet certain security and compliance criteria determined by the IT department.

Device Security Requirements

- Devices must have up-to-date antivirus software and security patches.
- Employees must use strong, unique passwords or passcodes to access devices.
- Devices must be configured to automatically lock after a specified period of inactivity.

Data Protection

- Employees must adhere to data classification policies and take necessary precautions to protect sensitive financial data.
- Company data should not be stored on personal devices unless authorized by the IT department.

Network Security

- Employees must connect to secure and password-protected Wi-Fi networks.
- Public Wi-Fi networks should be avoided when accessing company resources.

Software and Application Management

- Only authorized software and applications should be installed on personal devices.
- Employees are responsible for keeping software and applications up to date.

Compliance and Legal Considerations

Regulatory Compliance

- All activities conducted on personal devices must comply with relevant financial regulations and industry standards.

Monitoring and Auditing

- The organization reserves the right to monitor and audit personal devices for security and compliance purposes.

Employee Responsibilities

- Employees are responsible for the security of their personal devices used for work purposes.
- Promptly report lost or stolen devices to the IT department.
- Report any suspicious activity or security incidents to the IT department.

Termination of Access

Access to company resources via personal devices may be revoked at any time, especially in the event of a security breach or termination of employment.

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