BYOD POLICY

Current Version	Version 1.0	Drafted by	Tarun Agarwal
Effective Date	1 July 2025	Reviewed by	Tarun Agarwal
Next Review Date	1 July 2026	Final Approval by	Samuel John

1. Objective

This policy defines the acceptable use of personal devices (laptops, smartphones, tablets) for official purposes, to safeguard company data and ensure secure access to corporate systems.

2. Scope

This policy applies to all employees, contractors, interns, and third-party personnel of mistEO Pvt. Ltd. (will be collectively referred as 'associates' hereafter in this document) who access company systems using personal devices.

3. Eligible Devices

'Associates' may use the following personal devices for work:

- Smartphones (Android, iOS)
- Laptops (Windows, macOS)
- Tablets (Android, iOS)

Devices must be:

- Owned by the employee
- Running the latest or a secure operating system version
- In good working condition

4. Approval Process

- Associates must seek written approval from their manager/ IT SPOC before using a personal device for work.
- The device must be registered with IT and security configurations must be reviewed.

5. Acceptable Use

Associates may:

- Access email, calendars, company-approved apps, and files
- Connect to the corporate Wi-Fi and VPN (if required)

Associates must **NOT:**

- Store sensitive data locally unless encrypted
- Use personal devices to bypass company security protocols
- Download pirated or malicious software
- Share the device with unauthorized users (e.g., friends or family) when company data is accessible

6. Security Requirements

All personal devices must:

- Use a **secure password or biometric lock**
- Be **encrypted** (if the OS supports it)
- Have **antivirus or security software** installed and updated
- Enable **remote wipe capability** (e.g., through MDM or a secure container app)
- Be regularly updated with OS and application patches

Company has the right to:

- Audit devices for compliance
- Restrict access or revoke permissions if a device is deemed insecure
- Perform a **remote wipe of corporate data** in case of device loss, theft, or termination of employment/ contract

7. Privacy

- MistEO will only access company-related data on personal devices.
- Personal data such as private photos, messages, or apps will not be accessed unless legally required.
- However, if the device is involved in a security breach or investigation, more extensive access may be required.

8. Support and Liability

- The IT team may offer **basic support** (e.g., setting up VPN, email) but is **not responsible** for personal device hardware/software issues.
- Employees are responsible for the **maintenance, repair, and replacement** of their personal devices.
- Loss or theft of personal devices must be reported **within 24 hours**.

9. Termination or Exit

- Upon resignation, termination, or revocation of access, all company data must be deleted from the personal device.
- IT may assist in data removal or enforce remote wipe measures.

10. Policy Violations

Violations of this policy may result in:

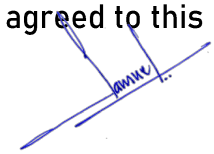
- Revocation of BYOD privileges
- Disciplinary action, including termination
- Legal action in case of data breaches or non-compliance with laws

11. Policy Review and Updates

This policy will be reviewed **annually** or when major changes in technology or regulations occur, with necessary approvals from CEO & CTO.

Acknowledgement

Associates must sign a BYOD Agreement acknowledging that they have read, understood, and agreed to this policy.



Signature:

Name: Samuel John

Employee ID: 001

Date: 1 July 2026

Samuel John

Digitally signed by Samuel John
Date: 2026.08.27 10:23:59 +05'30'