Acceptable Use Policy for Personal Devices

Kulture Reimagined Consulting

---

1. Purpose & Scope

This Acceptable Use Policy (AUP) outlines the guidelines for employees and contractors using personal devices (e.g., laptops, mobile phones, tablets) to access, store, or process company data. It applies to all personnel working with Kulture Reimagined.

---

2. Approved Personal Devices

Employees may use personal devices for business activities if they meet the following security requirements:

- Devices must have up-to-date operating systems and security patches.
- Multi-Factor Authentication (MFA) must be enabled for all company-related accounts.
- Devices must have password protection, encryption, and automatic lock settings enabled.

---

3. Security Requirements

To protect company data and intellectual property, employees must:

- Install and maintain antivirus and anti-malware software.
- Avoid storing sensitive company data locally on personal devices; instead, use Google Drive or other approved cloud storage.
- Report any lost, stolen, or compromised devices immediately.

---

4. Network & Internet Usage

Employees must:

- Use only secure Wi-Fi connections (no public or unsecured networks).
- Connect via a VPN when accessing company systems remotely.
- Avoid downloading unauthorized or unverified software that may pose security risks.

---

5. Data Protection & Confidentiality

- Employees must not share company data with unauthorized persons.
- Any sensitive client information must be accessed only through company-approved platforms.
- Company-related emails must only be sent from the official Google Workspace account.

---

6. Prohibited Actions

The following actions are strictly prohibited:

- Bypassing security controls or disabling antivirus software.
- Using personal devices to access company accounts on unsecured or shared devices.
- Installing unauthorized software that could compromise data security.
- Copying, downloading, or storing client information on unapproved platforms.

---

7. Incident Reporting

If a personal device used for work is lost, stolen, or compromised, employees must:

1. Immediately report the incident to Kulture Reimagined's designated security contact.
2. Change all company-related passwords associated with the affected device.
3. Perform a security check to ensure company data is not at risk.

---

8. Policy Acknowledgment & Agreement

All employees and contractors must read and acknowledge this policy before using personal devices for work. Non-compliance with these guidelines may result in restricted access to company resources or termination of contracts.

By signing below, I acknowledge that I have read, understood, and agree to abide by this Acceptable Use Policy for Personal Devices.

Employee Name: _____
Signature: _____
Date: _____