Definitions

Bring Your Own Device (BYOD): Any privately-owned wireless or portable device inclusive of laptops, tablets, mobile phones, and any other hand-held working equipment.

Overview

This policy outlines the acceptable use of personal devices at {COMPANY-NAME} to ensure secure access to organizational resources. It applies to employees, contractors, board members, volunteers, and other participants in the BYOD program. This program is intended to safeguard sensitive information from within the company from exposure intentionally or by mistakes.

Purpose

The rationale for this policy is to set the acceptable policy for the exercise of using personal gadgets when it comes to connecting to company systems, networks, or data. The policy safeguards {COMPANY-NAME} data integrity while allowing the flexibility of BYOD usage for legitimate business needs.

Scope

This policy applies to:

- Employees (full-time and part-time), contractors, and volunteers.
- Any personal device that accesses {COMPANY-NAME} systems, including laptops, smartphones, and tablets.
- All software and apps used to connect to company systems.

Key Security Risks

- **Device Loss or Theft:** The chances of losing sensitive data are high.
- **Malware:** Threats such as viruses or spyware that can harm company systems.
- **Unauthorized Access:** Threats by devices with poor security settings.
- **Compliance Breach:** Legal risks due to mishandling sensitive information.

Policy Details

- **Eligibility:** Only devices that have been approved by the IT department are permitted to connect to the company network.
- **Device Configuration:**

    - Must be protected using robust passwords, PINs, or biometric verification.
    - All devices are to have current operating systems and applications.
    - IT will configure devices with necessary software like VPNs and antivirus programs.
- **Usage Restrictions:**
    - Devices must not store sensitive data on unapproved platforms.
    - Jailbreaking or bypassing device security is prohibited.
    - Accessing or transferring data outside authorized networks is forbidden.
- **Data Management:**
    - All corporate data must be encrypted.
    - Personal devices are to follow company-approved backup protocols.

Responsibilities

- **Employees:**
    - Protect your devices and inform authorities of stolen or unauthorized access.
    - Follow the security protocols, usually periodic updates and password changes.
- **IT Department:**
    - Manage the approval of devices, track access, and implement security controls.
    - Install or configure security tools and perform audits to comply.

Incident Reporting

All losses or thefts and or incidents where an employee learns that their device has been compromised in any way must be reported to the IT department. Failure to take this measure may result in withdrawal of access or otherwise severe punishment.

Compliance

Failure to comply with the BYOD policy may lead to:

- Termination of device access privileges.
- Disciplinary actions, up to and including termination of employment.

Acknowledgment

By signing this document, I acknowledge that I have read, understood, and agree to comply with the {COMPANY-NAME} BYOD Security Policy.

Name: _________________________

Signature: ____________________

Date: _________________________