

\*replace with your company logo

BRING YOUR OWN DEVICE ( BYOD)

POLICY

# Purpose

\*COMPANY NAME HERE\* grants its employees the privilege of purchasing and using smartphones, tablets and laptops of their choosing at work for their convenience. \*COMPANY NAME HERE\* reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

The purpose of this policy is to provide guidance that protects the security and integrity of \*COMPANY NAME HERE\* data and technology infrastructure.

\*COMPANY NAME HERE\* employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the \*COMPANY NAME HERE\* systems.

# Scope

This policy is applicable to, and will be communicated to, all \*COMPANY NAME HERE\* users, contractors and third parties who interact with information held by

\*COMPANY NAME HERE\* and the information systems used to store and process it.

# Policy

**Acceptable Use**

Employees may use their mobile device to access the following company-owned resources:

Email Calendars Contacts Documents

# Devices and Support

Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.

Tablets including iPad, Android and Windows are allowed. Laptops including Mac and Windows are allowed.

Devices must be presented to \*COMPANY NAME HERE\* designated IT team for provisioning and configuration.

# Security

In order to prevent unauthorized access, devices must be password protected using the features of the device.

Passwords must comply with the \*COMPANY NAME HERE\* Password Policy. The device must lock itself with a password or PIN if it’s idle for five minutes.

The employee’s device may be remotely wiped if;

* 1. The device is lost,
  2. The employee terminates his or her employment,
  3. \*COMPANY NAME HERE\* detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

# Enforcement

While \*COMPANY NAME HERE\* will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc.

The company reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company’s acceptable use policy as outlined above.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Definitions

**Term**: Bring Your Own Device (BYOD)

**Definition**: A device used by an employee to access \*COMPANY NAME HERE\* resources but not owned by the \*COMPANY NAME HERE\*.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Note |
| 1.0 | 10/01/2021 | \*Your Name |  |
|  |  |  |  |