Business BYOD Agreement

This document establishes policies, rules of behavior, and standards regarding the usage of personal smart devices (phones, watches, or tablets, by **<Business Name>** employees to access the company's resources and/or services. For access to this material, employees are required to respect, read, sign, and follow **<Business Name's>** policies concerning using external personal devices for this purpose.

This bring your own device (BYOD) policy is intended to protect the security and integrity of **<Business Name's>** data and technology. Limited exceptions to this policy may occur due to specific variations in devices and platforms used for data access.

Expectation of Privacy

<Business Name> will respect the privacy of any employees using their personal devices to request access to company data and services. **<Business Name>** will also only request access to a personal device when a technician needs to implement security updates or controls or to respond to legitimate discovered requests that arise out of administrative, civil, or criminal proceedings. This differs significantly for any equipment provided to employees from **<Business Name>**. In this case, employees do not have the right, nor should they have any expectation, of privacy while using **<Business Name>** equipment and services.

Acceptable Usage

- **<Business Name>** defines any activity as acceptable business use when it directly or indirectly supports the business.
- **<Business Name>** defines acceptable personal use as any activity done on company time that may be considered reasonable and limited personal communication or recreation. This includes reading, texting, or game playing.
- Devices may not be used to:
  - Transmit or store illicit materials
  - Store or transmit any proprietary information
  - Engage in harassment of others
  - Engage in any business activities not associated with **<Business Name>**
- Employees of **<Business Name>** may use their personal smartphones and tablets to access the following resources owned by **<Business Name>**:
  - Email
  - Work contacts
  - Calendars
  - Documents
- **<Business Name>** has a zero tolerance policy in regards to dangerous activities while using accepted personal devices. This includes texting, chatting, or emailing while driving. When operating a vehicle, only hands-free talking is allowed.

Devices and Support

- Here's a listing of the devices that **<Business Name>** supports:
  - Device 1
  - Device 2
  - Etc.
- Insofar as connectivity issues, IT management will provide support. If there are hardware problems, please contact device support via the carrier or device manufacturer.
- All devices must be presented to the IT department for job provisioning and configuration of **<Business Name>**-approved apps. This includes browsers, office productivity software, VoIP software, productivity solutions, and security tools. All devices must be properly provisioned before being granted to **<Business Name's>** network.

Security

- In order to prevent security breaches, all devices must be passcode-protected or have a PIN approved by the IT department. This is required for **<Business Name>** network access.
- **<Business Name's password policy>**
- The device must automatically lock itself with a passcode or PIN when it's been idle for **<established>** minutes.
- Compromised devices such as rooted Android phones or jailbroken iOS devices are forbidden when accessing **<Business Name's>** network.
- Any smartphone or tablet that is considered strictly for personal use may not be used to access **<Business Name's>** network.
- Employee access to company data is limited and based on the user profiles defined by the IT department and will be automatically enforced.
- Personal devices may be automatically wiped if:
  - The employee loses the device or it's stolen
  - The employee terminates employment with **<Business Name>**
  - There is a data or policy breach
  - There is a virus or similar issue detected on the device

Risks, Liabilities, or Disclaimers

- IT will take every precaution to prevent the loss of personal data should a device require a remote wipe. Still, it is the employee's responsibility to prevent data loss by performing regular backups of materials like contacts, emails, and personal files.
- **<Business Name>** reserves the right to remotely disconnect any device from the network at any time without notification.

- Lost or stolen devices must be reported to **<Business Name>** within 24 hours of the incident. Employees are also responsible for notifying their carrier immediately upon loss.
- Employees are expected to use devices in a purely ethical manner at all times. They are also required to adhere to acceptable use policies by **<Business Name>**.
- Employees are responsible for any costs associated with their device.
- Employees assume full liability for any risks that might include, but are not limited to, the partial or complete loss of **<Business Name>** data or any personal data lost due to crashes, errors, bugs, viruses, software or hardware failures, malware, or any programming issues that may render the device unusable.
- **<Business Name>** reserves the right to take any appropriate disciplinary action, which may lead up to termination, for non-compliance with stated BYOD policy.

User Acknowledgement and Agreement

I acknowledge, understand, and will comply with the above referenced device security policy and rules of behavior, as applicable to my BYOD usage of **<Business Name>** services. I understand that business use may result in increases to my personal monthly service plan costs. I also further understand that reimbursement of any business-related data/voice plan usage of my personal device is not provided.

Employee Name: _____

BYOD Device(s): _____

Employee Signature: _____ **Date:** _____