**Mobile Device Policy**

**(Sample Template)**

*[IMPORTANT NOTE: The following Mobile Device Policy is a sample template provided by TRUCE Software solely as a courtesy and for informational purposes only. You should feel free adapt it to fit your particular organization. You may want to include additional details where it makes sense, or even add entirely new sections to address the needs of different work groups with varying job requirements. For clarity, however, TRUCE Software is not providing legal advice, or guaranteeing that all the terms outlined in this sample template are enforceable under applicable laws. You should consult with your own legal counsel if you intend to use this sample template to create and implement a mobile device policy for your organization.]*

**Last Updated: [DATE]**

This Mobile Device Policy (the “Policy”) is issued by [NAME OF COMPANY] (the “Company”), and outlines rules and policies for the use of Mobile Devices by Employees in the workplace or in the context of their employment with the Company.

1. **Defined Terms**.
2. “Company Device” means a Mobile Device that is owned by the Company and furnished by the Company to an Eligible Employee for Company business.

1. “Company Information” means data, trade secrets and intellectual property of the Company and other members of its corporate family.
2. “Company Vehicle” means a vehicle that is owned or leased by the Company.

1. “Covered Personal Device” means a Personal Device that is used by an Employee for Company business, or to access Company systems or Company Information.
2. “Eligible Employee” means an Employee who is eligible to use a Company Device or a Covered Personal Device for Company business, or to access Company systems or Company Information—based on the Company’s determination that such Employee has a legitimate business need to do so. For example, Employees who have the following types of job requirements are likely to be considered Eligible Employees:

* Employees who must be available to respond to internal or external requests from customers, suppliers or other business partners on a 24/7 basis.
* Employees who are listed as an emergency contact for the Company.
* Employees whose primary responsibilities require them to work outside of the office or Company premises but who need the ability to access Company calendars, emails, documents or other Company software or systems, as well as maintain timely communication with other Employees and/or customers in order to maintain productivity during the workday.
* [ADD OTHER COMPANY CRITERIA AS NEEDED]

1. “Employee” means an employee of the Company, whether such employee works on a full-time, part-time, project or temporary basis.

1. “Mobile Device” means a cell phone, smartphone, tablet or other portable electronic device with the ability to receive and/or transmit voice, text and/or data without a cable or wired connection.

1. “Non-Covered Personal Device” means a Personal Device that is used by the Employee for personal purposes only, and is not used for Company business, or to access Company systems or Company Information.
2. “Personal Device” means a Mobile Device that is owned by an Employee.
3. “TRUCE System” means the TRUCE Mobile App, the TRUCE Beacon, the TRUCE Management Console and associated software which are designed to provide protective measures to enhance safety in a vehicle, location or other environment.
4. **Scope of Policy**. This Policy applies to all Mobile Devices, whether they are Company Devices, Covered Personal Devices or Non-Covered Personal Devices.

1. **Company Support Program for Eligible Employees.**
2. Mobile Devices play an integral role in the Company’s operations and its ability to deliver “best in class” service to its customers.
3. The Company currently offers the following Mobile Device program to Eligible Employees:

[INSERT COMPANY PROGRAM DETAILS – e.g., providing Company Devices, paying for monthly service on Company DeviceS, providing a monthly allowance for Covered Personal Devices, etc.]

1. The Company will provide technical support and guidance for Company Devices and Covered Personal Devices relating to the installation and maintenance of Company-provided software and connection to the Company’s network resources. All other support issues must be directed to the mobile service provider.
2. **Rules for Different Classes of Mobile Devices.**

* 1. Eligible Employees who wish to use a Mobile Device for Company business, or to access Company systems or Company Information must agree to use either (i) a Company Device or (ii) a Covered Personal Device.

* 1. Company Devices:
* Company Devices: The Company may issue Company Devices to Eligible Employees to facilitate the conduct of Company business. Company Devices will remain Company property, however.
* If requested by the Company, Eligible Employees with Company Devices will be required to make the Company Devices available to the Company, including to facilitate upgrades, replacement and/or inspection.
* Eligible Employees must return all Company Devices to the Company if and when the period of employment ends for any reason.
* Loss or theft of any Company Device must be reported to the Company and to the mobile service provider within 24 hours.
  1. Covered Personal Devices:
* Covered Personal Devices: Any Eligible Employee who wishes to use a Personal Device for Company business may request written approval to do so from his/her manager.
* Any Eligible Employee who chooses to use a Covered Personal Device acknowledges that he/she is giving the Company control over certain aspects of the Covered Personal Device and agreeing to be subject to additional rules and restrictions, in exchange for access to Company resources (e.g., Company Information, Company network, Company email). These rules and restrictions include the following:
  + Eligible Employees are responsible for backing up any personal content on Covered Personal Devices and keeping Covered Personal Devices updated and in good working order.
  + The Company’s confidential or sensitive information should never be downloaded to or stored on any Covered Personal Device.
  + The Company will have no responsibility or liability for loss or theft of, or damage to, any Covered Personal Device.
  + Loss or theft of any Covered Personal Device must be reported to the Company and to the mobile service provider within 24 hours.
  1. Non-Covered Personal Devices: Employees are prohibited from using any Personal Device for Company business, or to access Company systems or Company Information, unless the Personal Device is a Covered Personal Device.
  2. Security:
* Employees must implement a PIN, password or other Company-approved security protocol on every Company Device or Covered Personal Device. When possible, Employees should use two-factor or two-step verification for added security [OPTIONAL].
* Eligible Employees are required to permit the Company to install Mobile Device Management (MDM) software on all Company Devices and Covered Personal Devices. This software will do the following:

[PROVIDE DETAILS OF YOUR MDM PLATFORM, IF APPLICABLE]

* Employees agree to maintain the original operating system on all Company Devices and Covered Personal Devices, and keep them current with security patches and updates, as released by the manufacturer. No Employee will “jail break” any Company Device or Covered Personal Device by installing software that allows any person to bypass standard built-in security features and controls.

1. **TRUCE System.**
   1. The TRUCE System is intended to increase employee safety and productivity. The core function of the TRUCE System is to disable certain functions on a Mobile Device (e.g., text messaging, email, internet browser) in certain situations (e.g., when the user is driving a vehicle).

* 1. The TRUCE System does not monitor (or permit the Company to monitor) the Employee’s communications or any other data or information on a Company Device, Covered Personal Device or Non-Covered Personal Device. This includes contacts, emails, photos, credit card information, app usage, internet browsing history, etc.

* 1. When active, the TRUCE System does the following:

[DESCRIBE WHAT APPS/FEATURES WILL BE ENABLED/SUPPRESSED FOR SPECIFIC WORK SITUATIONS]

* 1. The TRUCE Management Console will monitor usage of the TRUCE mobile app and will alert the Company if the TRUCE mobile app is no longer active on a required Mobile Device.

* 1. Eligible Employees are required to permit the Company to install the TRUCE System on all Company Devices and Covered Personal Devices.
  2. ***In addition, if any Employee wishes to have the ability to bring a Non-Covered Personal Device into (i) a Company Vehicle, (ii) a non-Company Vehicle for Company business, or (iii) any other Company workplace, the Employee will be required to permit the Company to install the TRUCE System on that Non-Covered Personal Device.***
* If an Employee is unwilling to permit the Company to install the TRUCE System on any Non-Covered Personal Device, then that Employee will be prohibited from bringing that Non-Covered Personal Device into any Company Vehicle, any non-Company Vehicle for Company business, or any other Company workplace; and, in addition, that Employee will be personally and financially liable if that Employee is involved in an accident and any Non-Covered Personal Device is determined to be a contributing factor.

1. **Acceptable and Prohibited Uses of Mobile Devices.**

* 1. General Use at Work: While at work, Employees are expected to exercise discretion in using Mobile Devices (whether they are Company Devices or Personal Devices).
* Employees should avoid using Mobile Devices for any personal use during work time. Excessive use of any Mobile Device for personal calls, texting, accessing personal apps or social media activity during the workday, regardless of the Mobile Device used, can interfere with the Employee’s productivity and also be distracting to other employees.
* Employee use of Mobile Devices for personal matters should be limited to scheduled breaks or lunch periods in non-working areas. Employees should ensure that their friends and family members are aware of this policy.
* Employees are prohibited from using any feature of any Mobile Device (including the camera, microphone or any app that accesses the camera or microphone) to record any of the Company’s confidential information—unless the Company expressly authorizes an Employee to do so in furtherance of that Employee’s work for the Company.
* Employees are prohibited from streaming, downloading or uploading any material which is illegal, obscene or inappropriate on (i) any Company Device or (ii) on any Personal Device which is connected to a Company network or other Company-controlled internet connection. For clarity, the Company’s policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to the use of Mobile Devices in the workplace and in connection with all work-related activities.
* The Company will have no responsibility or liability for loss of or damage to any Personal Device.

* 1. Unsafe Work Situations. In the interest of safety and minimizing distractions, Employees are prohibited from using Mobile Devices in any work-related locations in which the use of Mobile Devices may create an unsafe work environment or a distraction the Employee and/or other employees. For clarity, all of the following Company workplaces are deemed to be “unsafe work-related locations” where the use of Mobile Devices is always prohibited, unless the TRUCE System has been installed and is operational:

[INSERT LIST OR DESCRIPTION OF ALL WORK AREAS WHERE MOBILE DEVICES ARE ALWAYS PROHIBITED].

* 1. Mobile Devices and Vehicles. Mobile Devices can create special safety risks in a vehicle. For this reason, Employees are required at all times to comply with this Policy and obey all applicable laws relating to the presence and use of Mobile Devices in a vehicle. The following vehicle-specific rules apply to all Employees:
* The TRUCE System must be installed on all Mobile Devices that any Employee intends to bring into and/or use in (i) any Company Vehicle or (ii) any non-Company vehicle which is used for Company business. For clarity, this rule applies not only to Company Devices, but also to Personal Devices (*including Non-Covered Personal Devices*).
* Employees driving or operating any Company Vehicle are prohibited from using Mobile Devices, except that (i) voice calls may be made in “hands-free” mode if the calls do not create a safety risk or a distraction and (ii) Mobile Devices may be used in any otherwise-authorized manner when the vehicle is parked and the vehicle is turned off.
* Employees driving or operating any non-Company Vehicle for Company business are prohibited from using Mobile Devices, except that (i) voice calls may be made in “hands-free” mode if the calls do not create a safety risk or a distraction and (ii) Mobile Devices may be used in any otherwise-authorized manner when the vehicle is parked and turned off.
* Mobile Devices should never be used, viewed or accessed in a vehicle while held in the driver’s/operator’s hand (unless the vehicle is parked and turned off). “Hands-free” means just that—hands free.
* Hands-free voice calls should be as short as possible, to enable the driver/operator to remain focused on the primary task of driving/operating the vehicle. If a longer conversation is required while driving, Employees should find a safe location to park and turn off the vehicle.
* When communicating with an Employee who is driving/operating a vehicle, other Employees should avoid any non-essential interaction (e.g., calls, text messages, emails, etc.) with the Employee who is driving/operating a vehicle.
* These rules apply whether the desired use of the Mobile Device is for business or personal reasons, or whether the Mobile Device is a Company Device or a Personal Device.

[MODIFY THIS SECTION TO DEFINE THE SPECIFIC ALLOWABLE USES OF MOBILE APPS AS SUPPORTED BY TRUCE].

1. **Right to Monitor.** The Company retains the right to monitor Employees for excessive or inappropriate use of their Mobile Devices. If an Employee’s Mobile Device usage causes a decline in productivity or interferes with Company operations, that Employee will be prohibited from using Mobile Device in the workplace. Tampering or any attempt to tamper with the TRUCE System or any MDM software on any Mobile Device is strictly prohibited.
2. **Enforcement**: Violations of this Policy may result in disciplinary action, up to and including termination of employment, to the extent permitted by law.
3. **Right to Amend.** To the maximum extent permitted by law, the Company reserves the right to update this Policy at any time, with or without notice. A copy of the most current version of this Policy may be found on the Company’s intranet (currently available at [INSERT LINK]) or obtained from Human Resources.

1. **Agreement Required**: Written agreement to this Policy is required by each Eligible Employee prior to (a) receiving a Company Device or (ii) accessing Company Information or Company resources via a Covered Personal Device. However, if an Eligible Employee uses a Covered Personal Device for Company business prior to confirming his/her written agreement by signing this Policy, that usage of the Covered Personal Device will be treated as the Eligible Employee’s “agreement” to this Policy.
2. **Policy Acceptance (Agreement).** By signing below, I acknowledge that I have read and understand this Policy, I agree to comply with this Policy as it applies to my use of Mobile Devices in relation to my employment with the Company.

Employee Signature:

Employee Name:

Date: