

# **BYOD POLICY TEMPLATE**

## **I. PURPOSE**

The mass-adoption of employee-owned personal smartphone and tablet (mobile) devices has, we believe, increased productivity. but has also exposed individuals and businesses to new security risks. While the decision of <Your Law Firm> to allow its partners, associates, and staff to use their own mobile devices, in order to improve productivity and work efficiency, it does so ever-aware of the increased risk.

The purpose of this policy is to establish the criteria governing the authorized use of employee-owned (personal) mobile devices on <Your Law Firm>'s network, and with <Your Law Firm>'s clients' confidential data.

Employees may use registered personal mobile devices to access <Your Law Firm>'s database and approved internal wireless network as necessary, in the course of their normal business routines, in support of <Your Law Firm>'s published goals and objectives.

*Continued on next page*

## II. PERMISSIBLE USE

<Your Law Firm> defines the “permissible use” of personal mobile devices as activities that directly or indirectly support the business of <Your Law Firm>. <Your Law Firm> considers limited personal use of mobile devices on company time as acceptable, including limited personal communication or recreation. However, excessive personal calls, e-mails or text messaging during the workday, regardless of the device used, can interfere with employee productivity, be distracting to others, and is not permitted.

While at work, employees are expected to exercise the same discretion in using their personal mobile devices as is expected for the use of company devices. <Your Law Firm>’s policies pertaining to harassment, discrimination, retaliation, trade secrets, and confidential information apply to employee use of personal devices for work-related activities.

Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times. This includes the <Your Law Firm’s State> Rules of Professional Conduct, which apply to all activities of <Your Law Firm>, including any activities performed on your personal mobile device. Any activities that are not permitted to be performed under the <Your Law Firm’s State> Rules of Professional Conduct are strictly prohibited.

[Additionally, <Your Law Firm> strictly prohibits the installation or use of the following [apps]/[categories of apps] on any approved mobile device:]

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

*Continued on next page*

### **III. Registering Devices for Access**

All personal mobile devices used to access <Your Law Firm>'s network, resources, or clients' confidential data, must be registered with <Your Law Firm>'s [IT Manager]/[IT Department].

To comply with this policy, the mobile device user must agree to:

- Register the mobile device with <Your Law Firm>'s [IT Manager]/[IT Department].
- Activate native encryption system or purchase encryption applications or software to ensure all data on the mobile device is encrypted.
- Installation of <MDM Software Name>, <Your Law Firm>'s Mobile Device Management system, on the device (provided by <Your Law Firm>'s [IT Manager]/[IT Department]).
- Read, acknowledge and sign the Mobile Device Acceptable Use and Security Policy (this policy).

While <Your Law Firm> strives to allow as many different types of mobile device as possible to accommodate the preferences of its attorneys and staff, due to security issues, mobile devices no longer supported by their manufacturer with security, OS, and firmware updates will not be allowed to connect to <Your Law Firm>'s network.

*Continued on next page*

### **Duties and Responsibilities of the User:**

User agrees to a general code of conduct that recognizes the need to protect confidential data that is stored on, or accessed using, a mobile device. This code of conduct includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device;
- Maintaining the software configuration of the mobile device – both the operating system and the applications installed;
- Updating the mobile device operating system and applications on a regular basis;
- Preventing the storage of company data in unapproved applications on the mobile device;
- Ensuring the mobile device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes;
- Backing up all data, settings, media, and applications;
- Reporting a lost or stolen mobile device to the [IT Manager]/[IT Department] immediately; and
- Agreeing to random spot checks of mobile device configuration to ensure compliance with this policy.

Personal mobile devices are not centrally managed by <Your Law Firm>'s IT Services. For this reason, a support need or issue related to a personal mobile device is the responsibility of the mobile device owner. Specifically, the user is responsible for all costs associated with his or her mobile device.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the mobile device unusable.

*Continued on next page*

### **Duties and Responsibilities of <Your Law Firm>'s IT Manager:**

The following services related to the use of a personal mobile device are provided by <Your Law Firm>'s IT Services:

- Enabling the mobile device to access any web-based interface of the email system;
- Enabling the mobile device to access any web-based application system;
- Email, Calendar and Contact Sync service configuration;
- Installation, configuration and maintenance of any other apps designated for company use;
- Wi-Fi Internet Access configuration (this service is limited to the facility);
- Mobile devices not compliant with this policy will be unsubscribed from <Your Law Firm>'s network and data services.

*Continued on next page*

## IV. SECURITY REQUIREMENTS

The user is responsible for securing their mobile device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. <Your Law Firm> requires mobile devices to comply with the following security programs at all times:

- To protect against unauthorized access to the mobile device, devices must be password protected using the features of the device.
  - A strong password is required to access <Your Law Firm>'s network. For mobile devices, a strong password must be at least six characters or input points.
  - Mobile device passwords [are]/[are not] required to be changed [every [60]/[90]/[<enter value>] days, and cannot be any of the <value> previous passwords used].
- [<Your Law Firm> employs multi-factor authentication for access to its [network]/[designated mobile applications]. <Your Law Firm>'s multi-factor authentication system is operated by the [IT Manager]/[IT Department].]
- Your mobile device must be capable of encrypting all data stored therein, whether through native security systems, or a third-party security system installed by the user. The encryption system must remain active at all times.
- The mobile device must lock itself with a password or PIN if it is idle for five minutes.
- Anti-Brute Force attack systems that render the device inoperable or delete all data following 10 unsuccessful login attempts must be active.
- Rooted/jailbroken devices are forbidden from accessing <Your Law Firm>'s network.
- [To ensure the security of our clients' confidential information, <Your Law Firm> requires all authorized mobile devices to have [<enter MDM service>] Mobile Device Management software installed and operating at all times]
- [To ensure the security of our clients' confidential information, <Your Law Firm> requires all authorized mobile devices to have native security and mobile device tracking systems such as Find My iPhone or Android Device Manager to be active and registered with the [IT Manager]/[IT Department].]
- Removal of any native or installed security protocols is prohibited.

*Continued on next page*

## V. DATA POLICY

Registered mobile devices [must]/[should] be configured to keep <Your Law Firm>'s data segmented from the user's personal data at all times. <Your Law Firm> [has]/[has not] designated specific applications exclusively for business use. [Only approved mobile applications may be used for accessing, transmitting, or storing Confidential data.] [Use of approved mobile applications [for personal reasons]/[with personal data] is [strictly prohibited]/[is not recommended].]

Copying or transferring confidential data to [non-approved mobile applications or] non-approved devices is strictly prohibited.

User understands and accepts that <Your Law Firm>'s data stored on a registered mobile device will be removed remotely under the following circumstances:

- Mobile device is lost, stolen, or compromised (data breach, virus or malware, or other threat is detected);
- Mobile device belongs to a user no longer employed by <Your Law Firm>;
- Mobile device is found to be non-compliant with this policy;
- User decides to un-enroll from the Mobile Device Management system or other security system described in this policy; or
- User refuses to allow the [IT Manager]/[IT Department] to inspect the mobile device as required by this policy.

*Continued on next page*

## VI. EMPLOYEE PRIVACY

<Your Law Firm> makes every effort to respect the privacy of your personal mobile device. <Your Law Firm> will only request access to the mobile device to ensure compliance with this policy, to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

<Your Law Firm> has the right, at any time, to monitor and preserve any communications that use the <Your Law Firm>'s networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use. <Your Law Firm> reserves the right to review or retain personal and company-related data [on registered personal mobile devices]/[in all approved mobile applications installed on registered personal mobile devices]. <Your Law Firm> may review the activity and analyze use patterns and may choose to publicize these data to ensure that <Your Law Firm>'s resources in these areas are being use according to this policy.

<Your Law Firm> has agreed to the following specific provisions to ensure that personal privacy is protected:

[Provision 1]

[Provision 2]

[Provision 3]

*Continued on next page*



## VII. DISCLAIMER

This policy is intended to apply only to the use of registered personal mobile devices with <Your Law Firm>'s network and data, and does not apply to the use of any other types of equipment, or mobile devices owned by <Your Law Firm>.

This policy is intended to protect the security and integrity of <Your Law Firm>'s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms, and do not constitute a waiver of <Your Law Firm>'s right to enforce this policy. Acknowledgement and acceptance of the terms of this policy are required in order for any personal device to be connected to <Your Law Firm>'s network.

<Your Law Firm> reserves the right to disconnect devices or disable services without notification. While <Your Law Firm> will take every precaution to prevent personal data from being lost in the event it must remote wipe a registered mobile device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc. [<Your Law Firm> is not responsible for loss or damage of personal applications or data due to the installation, operation or removal of approved applications.]

<Your Law Firm> expects its attorneys and staff to use their personal mobile devices in compliance with all applicable laws. Employees who are charged with traffic violations or any other violation of applicable law resulting from the use of their personal mobile devices will be solely responsible for all liabilities that result from such actions.

Attorneys or staff who have not received authorization in writing from <Your Law Firm> and who have not acknowledged and signed this policy will not be permitted to use personal devices for work purposes. Failure to follow <Your Law Firm> policies and procedures may result in disciplinary action, up to and including termination of employment.

*Continued on next page*

## VIII. USER ACKNOWLEDGMENT AND AGREEMENT

I acknowledge that I have received, read, understand and will comply with the above listed terms and conditions for use of my personal mobile device to access <Your Law Firm>'s network and data. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided.

Employee Name: \_\_\_\_\_

Mobile Device: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_