

Sample Personal Mobile Device User Agreement

NOTE: This sample agreement should be reviewed and modified to fit the needs of your organization. Organizations should cross-reference with relevant existing policies where appropriate, comparing against relevant policies (e.g. mobile device and acceptable use policies) and ensuring terms are defined consistently across policies. Additional changes to this policy may be necessary to account for varying individual organizational security needs and user privacy expectations. **Delete this note before publishing.**

Purpose and Scope

This agreement between the user signing below and [*Organization Name*] (the “Organization”) is designed to balance the convenience of permitting personally-owned devices, including mobile devices, in the workplace against risks related to the security of confidential, personal, and proprietary information.

A “Personal Device” as used in this agreement is defined as any personally-owned computer or electronic storage device including, but not limited to, desktop PCs, laptops, smartphones, tablet computers, or flash or hard drives that might be used to connect to Organization networks or systems, or otherwise have access to, transmit, or store Organization information. Such devices can be used for email, file access, download, or transfer, remote desktop and VPN connections, accessing an Internet-connected hotspot, social networking, tweeting, and standard phone calls as well as text messaging.

Any user who seeks to use his/her Personal Device for any business-related reason that involves sensitive business data, including documents or data containing personally identifiable information, protected health information, or other similar information related to Organization clients/customers that if lost, misused, or disclosed without authorization, could have an adverse impact on the privacy interests or welfare of others, or confidential or proprietary information such as business, financial, and marketing strategies, must obtain prior permission from his/her supervisor, except where such information use is permitted or protected by the National Labor Relations Act or other law. In general, the same precautions and common sense expected of the Organization employees when using an organization-owned device must be exercised when doing the same on a Personal Device.

Expectation of Privacy in Personal Devices

The user agrees that he/she has read and fully understands Organization’s Acceptable Use and Personal Mobile Device Security Policies and further understands his/her obligations under those policies.

If the user uses his/her device for any business-related reasons, whether involving sensitive business information or not, the user further agrees that he/she waives any and all expectations of privacy with respect to any information that may be stored on or received by the Personal Device.

The user understands that [*Organization Name*] may take possession of the device from time to time for the purposes discussed in this agreement (or for other business-related purposes, such

as a forensics investigation related to a potential security breach). While in the Organization's possession, all information stored/received on the Personal Device may be accessed by the Organization. Notwithstanding the above waiver of privacy rights, [Organization Name] will make reasonable efforts to (1) provide notice in advance to the user regarding the date and time when the Personal Device will be required, (2) inform the user regarding the expected duration of time that the Organization will need possession of the Personal Device, and (3) avoid the access/review of users' personal, non-business-related information. The Organization and user understand, however, that some incidental review of users' personal information is likely.

The user agrees to provide the Organization with access to the Personal Device, with or without prior notice, from time to time and as needed in the sole discretion of the Organization, to perform certain actions related to the security of the Personal Device. The user further agrees to the following:

The Organization May:

1. In the case of a mobile Personal Device (e.g. a smartphone), install and/or configure the device such that it can be wiped remotely (e.g. a factory reset in which all data is deleted from the device), in the event that the mobile device is lost, stolen, or removed from service (e.g. the employee purchases a new device).
2. Verify the Personal Device is configured properly to maximize security and, if needed in the Organization's sole discretion, to reconfigure the device or disallow the use of the Personal Device for business-related purposes.
3. Verify that all software/firmware patches and updates have been installed and, if not, installing them.
4. Verify that the employee has not disabled the passwords feature and/or violated the Organization's Password Policy.
5. Scan the device for any unauthorized or otherwise high-risk applications and, if any are found, remove such applications.
6. Monitor the device as the Organization deems necessary, in its sole discretion.

The User Must:

1. Allow the Organization to take physical control of the Personal Device, and to provide all necessary passwords and/or access codes upon request, for the purposes of monitoring the device and/or investigations related to Organization's business.
2. Obtain written permission from his/her manager to use the Personal Device for work-related purposes, including access to email or the network.
3. Monitor patches and updates for software/firmware available for the device including any applications that are downloaded/installed on the device and install such patches and updates as soon after release by the manufacturer as practicable.
4. Use a strong password and automatic screensaver that activates automatically after 10 minutes or less to lock the device when not in use.

5. Provide FIPS 140-2 device-level encryption, and where appropriate, FIPS 140-2 end-to-end encryption, to safeguard the Personal Device and any Organization information transferred to and/or received by it.
6. Secure the Personal Device with anti-virus software approved by the Organization.
7. Use a strong password that complies with the Organization's Password Policy to protect company email accounts on the Personal Device.
8. Use extreme caution and comply with the safeguards in the Organization's Email Policy and its policies governing use of Personal Devices when opening electronic communication such as email or text messages, and any attachments to such messaging, received from unknown senders.
9. Use a password for the Personal Device that is different from the password used to access the Organization network or Organization PC and which complies with the Password Policy.
10. Not disclose the Personal Device password to any source or person, including fellow workforce members, friends, and family members.
11. Maintain the Personal Device in its original state by not modifying its operating system or "jail breaking" the device in order to bypass built-in security features and protocols.
12. Not download applications or software from any untrustworthy and/or unapproved source.
13. Only use an approved Personal Device with company approved and configured VPN software to access the Organization's VPN.
14. Not visit any pornographic, offensive, or otherwise undesired and questionable sites on the internet which may result in the introduction of malicious programs into the Organization's network or server.
15. Not intentionally or unintentionally download or transfer sensitive business data to the Personal Device, unless expressly authorized to do so or such information use is permitted or protected by law.
16. Report any lost or stolen Personal Device, or inadvertent disclosure or unauthorized access of the Organization's information, to a supervisor within one hour or as soon as practicable after discovery.
17. Fully comply with the Organization's Acceptable Use, Mobile Data Security, and Access Control Policies.

User Release of Liability

The user understands and accepts the risk that any information stored on the Personal Device, including personal information, may be lost or destroyed through the use of required third-party applications or by the Organization, either intentionally (e.g. remote wiping of a mobile Personal Device) or unintentionally (e.g. accidentally deleting files while in the Organization's possession). The user releases the Organization from any liability arising out of or related to damage to or loss of such Personal Device, damage to or loss of personal (non-business) information on the Personal Device, and any loss of use of the device. The user additionally releases the Organization from reasonable expenses related to any service charges or fees charged by a third-party related to the Personal Device. However, in the event that the Organization maintains possession of the Personal Device for more than two consecutive business days, the Organization agrees to reimburse the user for the pro rata share of service charges or fees charged by a third-party related to the device.

By signing below the user agrees that he/she has read, understands and agrees to abide by the terms of this agreement.

User Name: _____

BYOD Device(s): _____

Services to be Used: _____

Anti-Virus Software installed the on Device: _____

User Signature: _____ **Date:** _____

Supervisor Signature: _____ **Date:** _____