The following is a template designed to assist in the policy development governing the protection of company computer systems and assets. As with all templates, this document provides a basic framework for the broad topics for consideration. Footnotes provide prompts for other general considerations and points for discussion. Each organization has unique risks and considerations that necessarily require customization. For more information, contact Ron Raether at (949) 622-2722 or ron.raether@troutman.com, or Mark Mao at (415) 477-5717 or mark.mao@troutman.com.

# PERSONAL DEVICE USE POLICY
**Template**

| | |
|---|---|
| **Title:** Personal Device Use Policy | **Doc. No.** Insert |
| **Issued by:** (e.g., Corporate Compliance) | **Original Effective Date:** Insert Month/Year |
| **Approved by:** (e.g., Board of Directors) | **Last Review/Approval Date:** Insert Month/Year |
| **Replaces:** Insert | **Effective Date:** Insert Month/Year |
| **Cross-referenced Policies:** Insert | |

Insert Company Name ("Company") may provide its employees, contractors, consultants, temporary staff, and other third parties (collectively, "BYOD Users") who acknowledge and agree to the terms and conditions below, the opportunity to use their own computers, smart phones, tablets, and other devices for business purposes to access and use email and other authorized Company systems and information (collectively, "Company Data"). Access and use is subject to the following terms and conditions (collectively, "Terms and Conditions").

## PERSONAL DEVICE REQUIREMENTS

1. "Personal Device" means a computer, smart phone, tablet, or other device that is authorized to access Company Data or is used to backup any such device and is owned by a BYOD User and acquired voluntarily, without payment by Company and without any expectation of reimbursement for any costs related to the purchase, activation, operational/connectivity charges, service or repairs, or other costs that may be incurred related to the device or its use.[1]

2. The minimum security requirements ("Minimum Security Requirements")[2] for using a Personal Device are subject to change from time to time, but include the following:

   a. Password-protected[3] access;

[1] Due to the infinite number of different devices and variety of different operating systems, companies may want to consider limiting the types of devices they are willing to support.
[2] Company may have additional security requirements, if operating in a regulated industry (*e.g.*, healthcare) or an industry with its own self-regulatory requirements (*e.g.*, PCI)

b. A password/pin code must be entered on any Personal Device after, at most, fifteen (15) minutes of inactivity;

c. The BYOD User must maintain the original Personal Device operating system and keep the Personal Device current with security patches and updates, as released by the Personal Device manufacturer. The BYOD User will not "jail break" the Personal Device (installing software that allows the user to bypass standard built-in security features and controls) or otherwise modify the safeguards installed on the Personal Device by the manufacturer; and

d. The Personal Device must be encrypted and any resulting back-ups must also be encrypted.[4]

3. If a Personal Device becomes non-compliant with any of the Minimum Security Requirements, it must be remedied within a reasonable period of time, or the Personal Device will be blocked from access to Company Data, and the Personal Device may be remotely wiped (which will return it to factory default settings and may result in the deletion of personal information maintained on the Personal Device).

## CONNECTION CRITERIA

1. The following criteria will be considered, initially and on a continuing basis, to determine if the BYOD User is eligible to connect a Personal device to Company Data:

   a. Status as an employee exempt from overtime;

   b. Status as an employee paid monthly expense allowance;

   c. Sensitivity of data the BYOD User can access; and

   d. The BYOD User's compliance with the Terms and Conditions included herein, applicable Company policies, and technical limitations and other eligibility criteria established by the Company.[5]

## ACCEPTABLE USE

1. Do not allow third parties to access or use any Company Data on or through the Personal Device.

2. The Personal Device used to access Company Data must comply with the Terms and Conditions, along with all federal, state, and other applicable laws.

3. Company Data must only be stored on a Personal Device as necessary, and storage of any Company Data must be kept to a minimum.

---

(…cont'd)

[3] Depending on the nature of the information or any regulatory restrictions, strong passwords may be required.

[4] Certain industries might have technical or regulatory requirements for such encryption.

[5] The criteria listed here are provided as an example of items that should be considered prior to establishing a connection to a Personal Device. Additional conditions may be necessary or warranted based on Company's risk assessment or technical or regulatory environments. Consult counsel on questions related to this issue, including those related to labor requirements for overtime-related matters.

4. Unless permitted to do so by their supervisor, BYOD Users may not download, store, or transfer confidential or sensitive business data to their Personal Device. Confidential or sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual, outcome of a charge/complaint/case, the Company or third parties' proprietary information, or the Company's financial operations.

5. Upon direction by the Company, BYOD Users agree to delete any sensitive business files that may be inadvertently downloaded and stored on the Personal Device during the process of viewing e-mail attachments.

6. To access Company Data on a Personal Device, BYOD Users may be required to download and install specific applications or software. The Company shall not be liable or responsible for any viruses or any damages, loss of data, or any other costs or expenses incurred by BYOD Users arising from such downloads or installation.

## TRANSFERRED, LOST, OR STOLEN PERSONAL DEVICE

1. In the event a Personal Device is lost, misplaced, or stolen, BYOD Users must notify Insert Point of Contact (*e.g.*, Information Technology Manager) as soon as practical after the device is missing. The Company may take appropriate actions, at its discretion, to safeguard Company Data, including remotely wiping the device (which will return it to factory default settings and may result in the deletion of personal information maintained on the device).

2. In the event a Personal Device is (i) transferred to someone else for any reason, including a warranty replacement or for servicing by any person other than the Company's Information Technology Department, or (ii) discarded, deactivated, or its use is otherwise discontinued, notification must be provided to Insert the Appropriate Point of Contact (*e.g.*, Information Technology Manager) and any and all Company Data must be immediately and permanently deleted from the Personal Device before such transfer.

## TERMINATION

1. When BYOD Users terminate their relationship with the Company, BYOD Users must, prior to their final working day with the Company, submit their Personal Device (and any applicable passwords, if required) to the Company in order to: (i) remove any and all Company Data from the Personal Device; and (ii) delete Company Data from any backup systems maintained by the BYOD User. The Company may take appropriate actions, at its discretion, to safeguard Company Data, including remotely wiping the device (which will return it to factory default settings and may result in the deletion of a BYOD User's personal information maintained on the device) or seeking judicial intervention to compel submission of the Personal Device to inspection by the Company.

## ADDITIONAL TERMS AND CONDITIONS

1. The Company will not provide any technical or services support for personal applications or personal data on the Personal Device.

2. At the request of the Company, BYOD Users must immediately surrender physical possession of their Personal Device (and any applicable passwords) to the Company.

3. BYOD Users do not have a right of privacy nor should they expect privacy while using a Personal Device to access Company Data.[6] Any Personal Device is, at all times, subject to the Company's right to access the Personal Device, with or without notice, to monitor, investigate, review, delete, collect data, remotely wipe data, and/or remotely disable the Personal Device at any time and for any reason. This may include the ability to view applications on the device and the ability to identify the location of the device through location-based services. The Company will not be liable for the loss of any personal data arising from such actions. The Company may also, at any time and without notice, collect information from a Personal Device for litigation or law enforcement purposes. By accepting this policy, the BYOD User signing below consents to disclosing and monitoring of Personal Device usage, including the contents of any files or information maintained or passed through that Personal Device.

4. BYOD Users shall indemnify and hold the Company harmless from and against any and all claims, damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to or resulting from any non-compliance with the Terms and Conditions. The Company is not responsible for any damages, loss of personal data or content, or any other costs or expenses incurred by BYOD Users relating to the Personal Device.

## BYOD USER ACKNOWLEDGEMENT AND AGREEMENT

It is the Company's right to restrict or rescind Personal Device privileges, or take other administrative or legal action due to failure to comply with the above Terms and Conditions. Violation of these rules may be grounds for disciplinary action, up to and including removal.

I acknowledge, understand, and will comply with this policy and Terms and Conditions, as applicable to my use of a Personal Device.[7] I understand that addition of Company-provided third-party software may decrease the available memory or storage on my personal device and that the Company is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third party software or use of the device in this program. I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by the Company. I understand that business use of a Personal Device may result in increases to my personal monthly service plan costs. I further understand that Company reimbursement of any business-related data/voice plan usage of my Personal Device is not provided.

Should I later decide to discontinue my use of a Personal Device, I will allow the Company to remove and disable any Company-provided third-party software and services, and Company Data from my Personal Device.

BYOD User Name: _____

BYOD User Signature: _____

Date: _____

[6] This area presents a great opportunity to proactively discuss the roll out and communication of the policy, which should include BYOD Users' expectations and what the Company can/should do when it comes to information access. Experience counts here.

[7] Effective policies require thorough training to educate users on policies, device access, and device security. Companies may want to consider implementing training for BYOD Users to help such users truly understand the purpose and elements of this policy.