**Company Name**

**BYOD Mobile Device Management Standards**

August 8, 2023

*This draft policy template is provided by Crosslake Technologies to serve as a starting point for your mobile device management (MDM) policy. You should review this policy with your IT security team and HR and legal advisors – then customize to your company’s specific needs.*

**Document Control**

|  |  |  |
| --- | --- | --- |
| **Date:** | **Person** | **Summary of Change** |
|  |  |  |
|  |  |  |
|  |  |  |

This document contains confidential information specific to COMPANY NAME’S business practices and should not be duplicated, used, or disclosed in whole or in part without prior written permission.

**Table of Contents**

[Overview 4](#_Toc142398068)

[Scope 4](#_Toc142398069)

[Acceptable Use 4](#_Toc142398070)

[Standards 5](#_Toc142398071)

# Overview

Mobile devices allow a greater level of flexibility and productivity – but the convenience of these devices carries more risk. The increased processing and storage capacity of mobile devices makes it easy for users to transmit or store large amounts of confidential data. As a result, we need to give special consideration to the use of mobile devices.

# Scope

This document establishes standards for employee / associate use of “bring your own device” (BYOD), personally-owned electronic devices for work-related purposes. BYOD personal devices include, but are not limited to: personal laptops, home desktops, notebooks, PDAs, smart phones and USB drives capable of storing or transmitting confidential company data.

Company policies require that rules for the acceptable use of workstations and mobile devices be identified, documented and implemented. Mobile devices used for work-related purposes must include appropriate technical and physical safeguards. Mobile devices that are not issued by the company are not permitted to connect to the company domain or applications, with the exception that associates with non-disclosure agreements may connect to an active company email account. Email must not be used to send confidential information unless it is encrypted. The use of personal mobile storage media devices to access other company resources is prohibited unless it is approved by IT management.

This document is part of the company’s cohesive set of security policies. Other policies may apply to the topics covered in this document, and as such, the applicable policies should be reviewed as necessary.

# Acceptable Use

The use of personal mobile devices to transmit or store company data is prohibited unless it is approved by IT management. Approval will generally require demonstration of a business need and review to determine that the device includes encryption capabilities, password protection, screen locks and antivirus software.

The company will respect the privacy of employees’ personal devices and will only request access to a device to implement or verify security controls or to respond to legitimate discovery requests arising out of administrative, civil or criminal proceedings. Company also reserves the right to “wipe” a personal mobile device of all company data or information when employment ends.

Confidential information stored on personal mobile devices must be removed as soon as it can be transferred to a secure, company-managed storage area.

It is the responsibility of any employee who is connecting to the Company network via a mobile device to ensure that all components of the remote connection remain secure. It is imperative that any mobile device used to conduct Company business be utilized appropriately, responsibly and ethically. Failure to do so may result in immediate suspension of that user’s account. The company may conduct periodic reviews to ensure policy compliance.

# Standards

* Personal devices connecting to company resources must include password protection and screen locking – or use other authentication requirements that may be established by the Company’s IT department.
* General access to the internet by personal mobile devices through the Company’s wireless guest network is permitted. However, an employee using the internet for recreational purposes through company networks must not violate any of Company’s internet-related acceptable use policies.
* Employees using mobile devices and services for remote access will, without exception, use secure remote access procedures (such as the use of an encrypted communication channel or a VPN to establish an encrypted connection) and use any other security measure deemed necessary by the Company IT department.
* Mobile devices are not to be left unattended when remotely connected to the company network or applications.
* Mobile devices should be kept in secure locations and out of public sight when not in use. Mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in a lockable compartment, such as a glove box, or in a trunk.
* Mobile device users must deactivate their devices when not in use in order to mitigate inappropriate use.
* Mobile device users must permanently erase company-specific data from their device as soon as it can be transferred to secure company storage systems, when its use is no longer required, or upon termination of the employee’s employment or contract.
* The cost to replace a lost or stolen mobile device is the responsibility of the employee.
* The mobile device user must immediately report any incident or suspected incidents of unauthorized access and/or disclosure of company information.
* The mobile device user also agrees to and accepts that his or her access and/or connection to Company’s networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.