Information Technology Department

Mobile Device Management Policy

November 15th, 2012

Version 1.0

Table of Contents

1 Overview

Tuolumne County is committed to equipping staff with the most appropriate mobile devices, to enhance their productivity and performance in the role of providing public service. The purpose of the Mobile Device Management (MDM) Policy is to establish the rules which will govern the use of mobile handheld computing devices to access County network resources.

1.1 Mobile Devices

Mobile handheld computing devices - such as iPhones, Androids and Tablets, are becoming increasingly powerful and affordable. Their size and function make them an excellent choice for staying connected to the workplace while on the go; however, it's this very portability that places the storage and transmission of confidential data at risk.

1.2 Scope

This policy applies to both County issued and Personal devices, and pertains to all employees requesting mobile device privileges.

1.3 Policy Revision

The MDM Policy will be reviewed/updated on an as-needed basis. Failure to accept any updated terms will result in the revocation of employee mobility privileges. Employees will be notified via email when policy update has occurred.

2 Services Available

Employees may use their mobile device to access the following County network resources:

2.1 Email

Access to County email, including calendars, contacts and tasks, will be provided as follows:

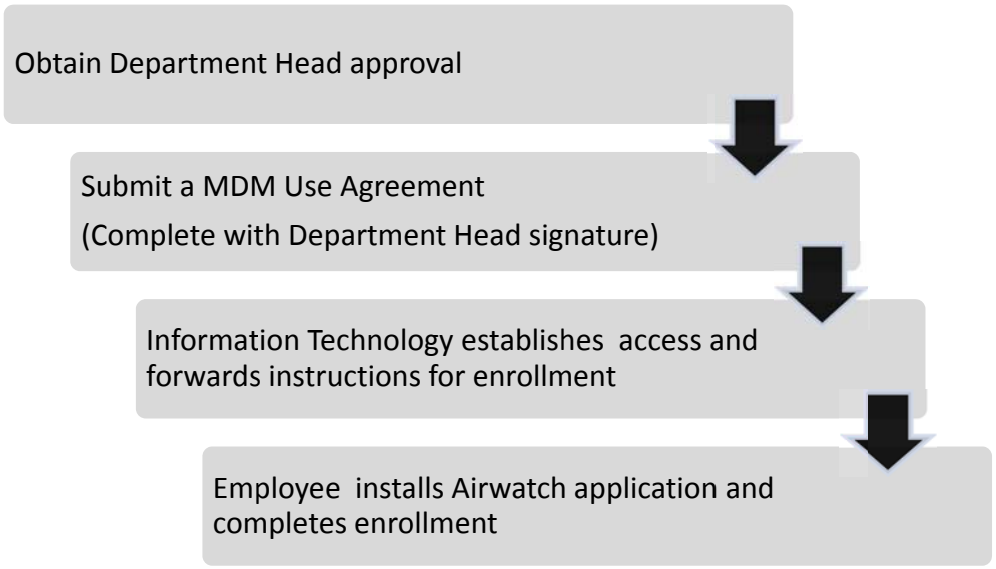
- The most recent one (1) day's email will be synchronized to the mobile device
- Calendars and contacts will synchronized to the mobile device
- Email cannot be moved from the County mail account to other accounts/applications residing on the mobile device

2.2 Wi-Fi Access

A number of County facilities currently have a wireless infrastructure in place. In the interest of reducing data plan usage, this connectivity will be extended to authorized users where possible.

3 Requesting Mobility Privileges

The process for requesting mobile device access to County network services is as follows:



4 Authorized Devices

4.1 Supported Devices

The County will only support the following devices:

- Apple iPhone, iPad and iPod Touch
- Android Phone and Tablet
- Windows Phone

4.2 Supported Operating System Versions

The following Operating System (OS) versions are required:

Device Type	Minimum OS Level
Apple iPhone, iPad and iPod Touch	5.0.0
Android Phone or Tablet	3.0
Windows Phone	8

5 Device Compliance

As a condition of being granted mobility privileges, employees agree to the installation of the following components, the associated restrictions and controls they establish and the impact they have on the use and behavior of your mobile device. County assumes no liability for loss of data or functionality.

5.1 AirWatch Application

A core component of County MDM Policy, the *AirWatch* application provides compliance monitoring and enforcement of security policies; further, installation is a prerequisite for enrollment. There is no cost for this application and instructions for installation will be provided by Information Technology.

5.2 NitroDesk TouchDown

TouchDown is an application required to enforce security policies and secure ActiveSync connections between Android devices and the County's email server. Employees who have opted to use Android devices will be required to purchase a license for *NitroDesk TouchDown*. Instructions for purchasing and installing this application will be provided by Information Technology.

5.3 Auto Lock

All devices will be set to auto-lock, and the display turned off, upon 5 minutes of inactivity.

5.4 Passcodes

All devices will require at least a 4 digit passcode. Passcodes must be kept confidential and are not to be shared. After 15 minutes of inactivity, the passcode will be required to unlock the device.

5.5 Device Sharing

Upon enrollment, mobile devices become a dedicated device for use by a single individual. The device is not to be shared or used by anyone other than the authorized employee.

6 Compromised Devices

Devices that have been *Rooted* (Android), *Jail Broken* (Apple) or otherwise modified will be considered compromised. Attempting to access County resources from a compromised device is strictly forbidden.

7 Device Loss or Theft

In the event that a mobile device has been stolen or lost, Information Technology must be notified within 24 hours. To report this, please contact the IT Exchange by sending an urgent email to itexchange@co.tuolumne.ca.us, or by calling (209) 536-2365. Information Technology will take appropriate measures to protect County information that may be on the device. Steps for remediation are dependent upon device type:

7.1 Personal Device

An *Enterprise Wipe* will be performed. Only County information, email and profiles will be remotely removed from the device. Personal information and applications will be left intact.

7.2 County Issued Device

A *Device Wipe* will be performed. All information, email, applications and profiles will be remotely removed from the device. The device is returned to its factory default configuration.

8 Employee Departure

Upon notification by Human Resources of employment termination, Information Technology will perform the following:

8.1 Personal Device

An *Enterprise Wipe* will be performed. Only County information, email and profiles will be remotely removed from the device. Personal information and applications will be left intact. Enrollment of both the employee and device will be cancelled.

8.2 County Issued Device

An *Enterprise Wipe* will be performed. All County information associated with the employee, such as email, applications and profiles, will be remotely removed from the device. Enrollment of both the employee and device will be cancelled. Transfer of this device to another County employee will require the approval and submission of a new *MDM Use Agreement*.

9 Enforcement

Any employee found to be in violation of this policy will have their mobility privileges revoked and may be subject to disciplinary action.

Tuolumne County Information Technology Department
Mobile Device Management – Use Agreement

All Network access is controlled by the County Administrative Officer through the Division of Information Technology in order to protect data integrity, confidentiality and insure Tuolumne County meets the legal requirements of its various hardware and software licenses. This form must be submitted for all individuals requesting mobility privileges to County network resources.

Request Summary

Date Of Request: _____

❑ New Request ❑ Device Replacement ❑ Services Add/Delete ❑ Employee Relocation

User Information

Last Name: _____ First Name: _____ Middle Initial: _____

Existing Username: _____ Job Title: _____

Department/Division: _____ Location: _____ Phone: _____

Device Information

❑ Apple iPhone
❑ Apple iPad
❑ Apple iPod Touch
❑ Android Phone
❑ Android Tablet
❑ Windows Phone

❑ Personal Device ❑ County Issued Device

Model: _____

OS Version: _____

** Note: Only one mobile device may be enrolled

Requested Services

❑ County Email

❑ County Wi-Fi (Not available at all locations)

❑ Other: _____

_____

❑ I hereby acknowledge that I have read, accept and will abide by the Tuolumne County Mobile Device Management Policy:

_____ _____
User's Signature Date Department Head Signature Date

_____
Department Head's Name (Printed)

Completed form may be emailed to ITExchange@co.tuolumne.ca.us, faxed to (209) 536-2361 or sent to IT via interoffice mail.
Please retain a copy for your records.

Mobile Device Management – Use Agreement Revised November 15, 2012