Document Type:	Regulation
Number:	4.30k
Effective:	08-25-09
Revised:	05-12-10
	03-07-11
	02-24-14
Legal References:	

MOBILE DEVICE TECHNICAL SUPPORT

I. INTRODUCTION

The scope of Information Technology's (IT) technical support for mobile devices is described in this regulation. Because the City has a provision for employees to use City-owned and/or City-authorized employee-owned mobile devices for City business, IT is responsible for the limited support of these devices as defined in this regulation. This regulation also defines the employee's responsibility related to these devices. This regulation applies to all departments in the City.

II. SCOPE OF SUPPORT:

A. Services and features:

1. Synchronization of mobile devices for the following City of Boise data:
   - Calendar
   - Contacts
   - Email

2. Access to:
   - Certain network drives (individual H: drive and department I:drive)
   - Internal city web-sites (current site security still applies)

3. Mobile applications approved for a legitimate business purpose by the employees department and/or IT and specifically designed for use on mobile devices.

   Devices that have been jail-broken or rooted will be restricted from services 1-3 listed above due to the network security vulnerabilities that represents.

4. City of Boise webmail for all mobile devices.

B. Device operating systems included:
   - Android (current major release minus one)
   - iOS (current major release minus one)

C. Device brands and models:
Any mobile device capable of utilizing services as described in this regulation, within the listed operating systems.

III. LICENSE OWNERSHIP:

City of Boise will purchase and own all Mobile Device Management licenses for synchronizing and accessing city data; licenses cannot be purchased and owned by individual employees for use on the City's network.

IV. DELETION OF DATA ON A MOBILE DEVICE

City data remains the property of the City of Boise. Employees opening, saving, storing or forwarding City data from a mobile device should exercise great care in protecting the City's property. Subject to the conditions below, IT may be required to reset a device, or remove city data, in certain circumstances. Resetting a city-owned device will completely restore the device to its original factory settings. Removing city data from an employee-owned device will only remove the city data that was allowed through the mobile device management system; the device itself will not be reset. IT will only perform these actions if necessary for technical support of the device and/or to maintain security and confidentiality of the city's data. This applies to both city-owned and employee-owned devices.

City of Boise data will be removed from an employee-owned device via the Mobile Device Management system; city data will be removed from a city-owned device by a complete device reset under these conditions:

A. Separation of employment:

Upon separation the employee's manager is responsible to ensure the device has been returned and/or reset.

B. Stolen or lost device:

If the device has been stolen, the employee is required to report this immediately and IT will immediately perform the steps necessary to delete city data. If the device has been lost, the employee will be permitted two (2) business days to locate the device. If the device has not been located after the allowed time, IT will perform the steps to delete the city data.

V. INDEMNITY

By utilizing the services described in Section II, the employee acknowledges the City of Boise is not responsible for the loss of personal data or damage incurred as a result of providing technical support to the device.

VI. PRIVACY

The City of Boise does not collect personal information on employee-owned devices such as personal passwords, applications or their use, email, text messages, call history, data usage, browser use, current location information or history.

City owned devices will have the following collected: installed applications, call history, data usage (not browser history), text messaging usage (not actual content of text messages), and location information. This information will not be viewable by IT staff without management authorization.

For enrollment in the Mobile Device Management system, the following device information is required: Device, brand, model, serial number, UID, Operating system, phone number (if applicable), and service provider.

VII. EMPLOYEE RESPONSIBILITIES

A. Must obtain authorization from management to utilize the described mobile devices services; this applies to both city-owned and employee-owned devices.

B. Must obtain authorization from management for the department to purchase a Mobile Device Management license or confirm an existing department-owned license is available for transfer to another employee.

C. Must ensure the device is enrolled in the standard city Mobile Device Management system (for services listed in Section II. Part A, 1-3).

D. Must ensure the device has the correct operating system and version.

E. Must immediately report to management if the device is stolen.

F. Must report to management within 2 (two) business days if the device is misplaced.

G. Must establish a password on the device to help ensure data security.

H. Must ensure a city-owned device is backed up daily as technical support may lead to the loss of data. Employees may contact the help desk for assistance.

I. Employees are also advised to backup employee-owned devices as technical support may lead to the loss of data.

J. Must contact the service provider directly to obtain support for all other services and features not described in this regulation.