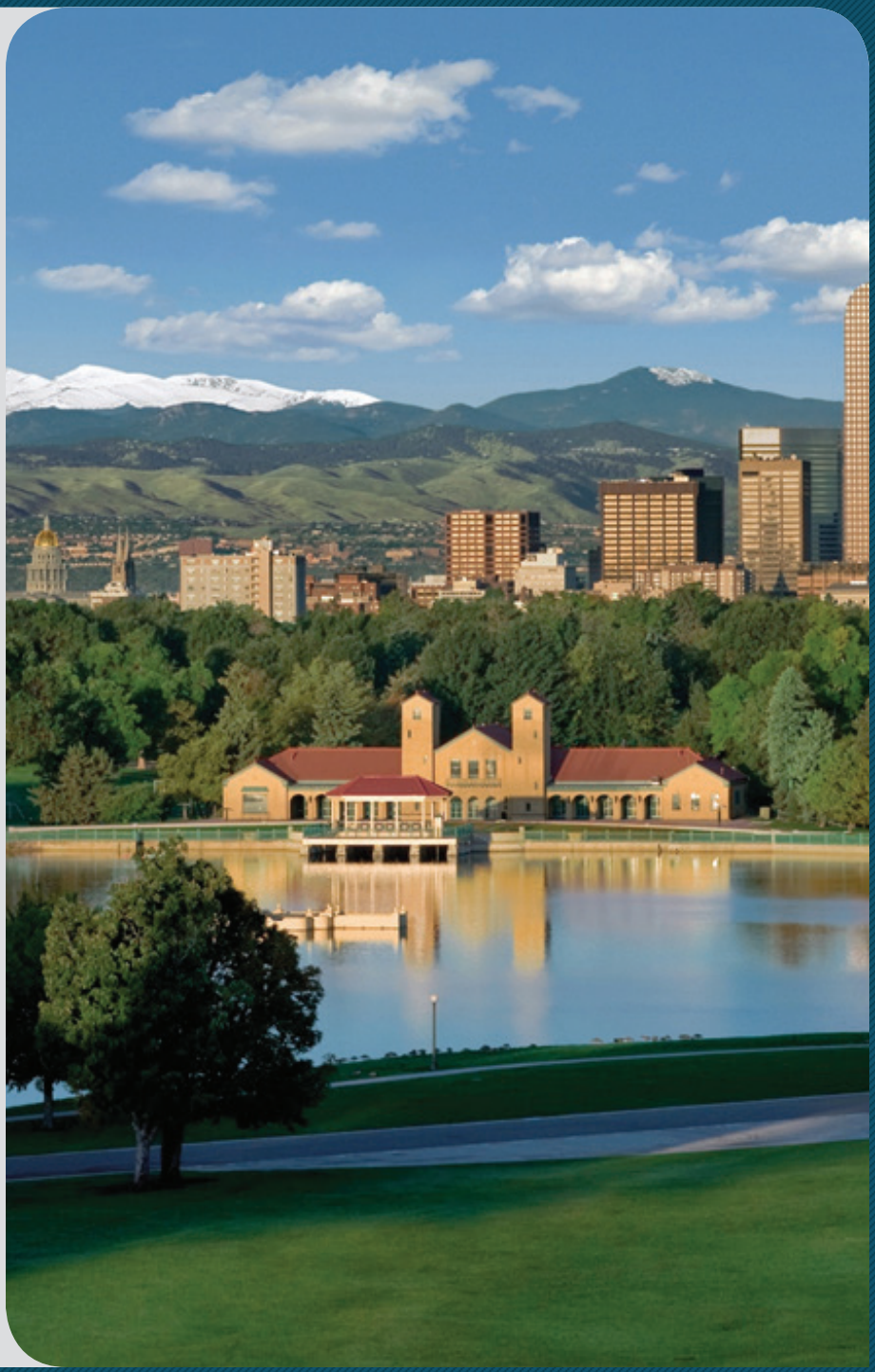
FOLLOW-UP REPORT
Mobile Devices
July 2016



Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor

The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver's government. He also chairs the City's Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City's finances and operations, including the integrity of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor Kip Memmott, MA, CGAP, CRMA, Director of Audit Services

Audit Staff

Shannon Kuhn, CISA, Audit Supervisor
Nick Jimroglou, CISA, Lead Auditor
Karin Doughty, CISA, Senior Auditor
Tyler Kahn, Senior Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ◆ Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
Report number: **A2014-001**

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202

720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

Timothy M. O'Brien, CPA
Auditor

July 7, 2016

Mr. Scott Cardenas, Chief Information Officer
Technology Services
City and County of Denver

Re: Audit Follow-Up Report

Dear Mr. Cardenas:

In keeping with generally accepted government auditing standards and the Audit Services Division's policy, as authorized by D.R.M.C. § 20-276, our Division has a responsibility to monitor and follow-up on audit recommendations to ensure audit findings are being addressed through appropriate corrective action and to aid us in planning future audits.

This report is to inform you that we have completed our follow-up effort for the Mobile Devices audit issued August 15, 2014. Despite the Technology Services department's efforts, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. As a result, the Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

For your reference, this report includes a Highlights page that provides background and summary information on the original audit and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation.

This concludes audit follow-up work related to this audit. I would like to express our sincere appreciation to you and to Technology Services personnel who assisted us throughout the audit and follow-up process. If you have any questions, please feel free to contact me at 720-913-5000 or Shannon Kuhn, Internal Audit Supervisor, at 720-913-5159.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

REPORT HIGHLIGHTS

Mobile Devices
July 2016

Status

The Technology Services department (Technology Services) has implemented nine of the fifteen recommendations made in the August 2014 audit report.

Background

Mobile devices are wireless portable devices that allow users to access data and information on the City's network. Cell phones, smart phones, and tablets are all mobile devices. The City hosts nearly 3,000 smart phones and more than 500 tablets for business use. The wireless voice and data usage budget for mobile devices managed by Technology Services is $1.3M for 2014.

Purpose

The purpose of the audit was to assess the effectiveness of Citywide mobile device administration and management, including determining whether: 1) performance measures are developed, implemented, monitored, and aligned with best practices; 2) mobile device access provisioning and de-provisioning is effectively performed; 3) security requirements are enforced; 4) lost and stolen devices are disabled and City data is deleted; and 5) wireless service payments are monitored and appropriate.

Highlights from Original Audit

The audit found that improvements needed to be made to the City's mobile device management governance with regard to financial monitoring, mobile device administration, and effective use of technology. Specifically, we identified the following:

- Technology Services needed to improve efficiency and security by:
  - Providing training and using the security features available in the City's mobile device management software
  - Removing City data from devices that were lost, stolen, or belonged to former employees
  - Incorporating best practices, legal opinions on privacy, regulations, and standards into mobile device policies
- Technology Services and agency liaisons needed to realize cost savings by:
  - Improving monitoring of usage, device inactivity, and payments
  - Reviewing wireless detail reports for accuracy
  - Monitoring under-utilized City-owned devices and suspending wireless service to those devices not being used, where applicable
  - Suspending wireless accounts for terminated employees timely
  - Preventing employees from receiving stipends for business use of personal mobile telephones while concurrently using City-issued mobile telephones
  - Removing unused and former employee devices from the monitoring software to avoid unnecessary license fees

Findings at Follow-up

Technology Services had developed procedures for mobile device handling that includes lost or stolen equipment, detection to ensure employees do not receive a stipend and have a City owned device, and a security incident process. Training has been provided to improve the use of mobile device management software. A risk assessment was performed to determine the need for software configuration changes. However, six out of fifteen (40 percent) recommendations have not yet been implemented due to a decision to use another application for management of mobile devices. Former employees may retain regulated or sensitive data on their personal devices after separation from the City, as data is not wiped from personal devices. Additionally, the Mobile Device Policy and the Acceptable Use forms that describe the use and safeguarding of mobile devices have yet to be implemented.

For a complete copy of this report, visit www.denvergov.org/auditor
Audit Contact Person: Shannon Kuhn |720.913.5159| Shannon.Kuhn@denvergov.org

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
Finding: Governance over Mobile Device Management Needs To Be Improved to Increase Security and Reduce Costs			
1.1	Technology Services should revise its Mobile Device Policy to meet information security requirements and modify its procedures accordingly.	Technology Services performed a risk assessment of two different software tools that could be used to enhance security within the City's mobile device environment. Based on cost, resources, re-configuration, and continued administration, Technology Services determined that Microsoft's Office 365 Mobile Device Management capabilities will be most cost effective. Technology Services is currently creating a Mobile Device Management policy, which includes the governing business rules for mobile devices by Office 365. Technology Services did not provide a date for completion for the policy.	**Agree/Not Implemented**
1.2	Technology Services should immediately begin removing City data from mobile devices reported lost or stolen and from devices belonging to former employees.	The Mobile Device Management policy is in the process of being created, which will not include a formal process for wiping City data from former employees' devices. Technology Services accepts the risk by allowing former employees to retain email on their mobile devices.	**Agree/Not Implemented**
1.3	Technology Services should consider enabling the containerization feature in the MDM software to segregate City data from personal information contained on the same device. This would allow removal of City data while preventing personal data from being wiped.	Technology Services analyzed containerization functionality and determined that it is not user friendly and not a viable option for the City.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.4	Technology Services should develop, document, and implement procedures for mobile device security incident response.	Technology Services has not put in place any technology-based controls to filter out sensitive or confidential City data when a personal mobile device is lost or stolen, or when an employee separates from the City. Technology Services has developed and documented a process for responding to mobile device security incidents, including a non-technical control for determining whether the lost, stolen, or former employee's device contains confidential or sensitive information. However, this step in the process has not yet been implemented. Technology Services also discourages employees from putting sensitive information on their personal devices, but we do not consider this a sufficient control.	**Agree/Not Implemented**
1.5	Mobile Device Management (MDM) software administrators should disable mobile device accounts for former employees immediately upon departure from the City to ensure security of City devices and eliminate unnecessary costs associated with the former employee's mobile device.	We found that email accounts are being disabled for former employees when they separate from the City. However, emails that reside on a former employee's personal device are not being wiped from the device, so emails that may contain sensitive information remain accessible to the employee after separating from the City.	**Agree/Not Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.6	Technology Services should, in consultation with the City Attorney's Office, create a Mobile Device Acceptable Use form that clearly states the City's rights and responsibilities in protecting its data. The form should clearly inform prospective users that their personal mobile device will have its data remotely removed if Technology Services determines that protected or sensitive data might be compromised. A signed copy of this form should be retained.	Technology Services met with the City Attorney's Office in September 2015 to discuss privacy sections of the Mobile Device Management (MDM) policy and the Acceptable Use Agreement. Discussions with the City Attorney's office are still in progress. Technology Services anticipates that the Mobile Device Acceptable Use form will be completed by the end of August 2016.	**Agree/Not Implemented**
1.7	Technology Services should comply with the City's Mobile Device Policy by not allowing mobile device access to City resources before receiving an authorized Financial Options Form. To help enforce this requirement, Technology Services should configure the MDM software to prevent mobile device access prior to approval.	At the time of the audit, Technology Services allowed users a ten-day temporary connection for mobile devices without approval. Rather than discontinuing this grace period, Technology Services reduced it from ten days to four days. Technology Services believes that this shorter grace period will mitigate much of the risk associated with the ten-day grace period while still allowing individuals to upgrade or change devices over the weekend or on holidays without interruption to service. Further, still allowing a grace period alleviates a high call volume to the service desk.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.8	Technology Services should update the City's Mobile Device policy to include critical requirements of standards. End users who work with protected data need direction on how to protect information on their mobile devices to comply with standards, laws, and regulations. Technology Services should document whether or not it is appropriate for employees who work with protected data to download sensitive information to their mobile devices.	Technology Services is in the process of creating the Mobile Device Management Policy, which will cover critical requirements and standards regarding the protection of City data.	**Agree/Not Implemented**
1.9	Technology Services should perform formal risk assessments for mobile devices at least annually.	A Mobile Device Management Risk Assessment process was created on July 29, 2015. Based on auditors' review of the risk assessment it appears that Technology Services has evaluated some risks associated with mobile devices. However, certain risks, such as allowing former City employees to retain sensitive information on their personal mobile devices, were not addressed other than high level.	**Implemented**
1.10	Technology Services should provide Agency liaisons with low- and zero-usage information at least monthly. Reviews should include data and voice usage for low, as well as zero usage. Information obtained from these low- and zero-usage reports should be used to communicate deactivations of mobile devices to eliminate unnecessary costs associated with inactive or low-usage mobile devices.	Technology Services has enabled software settings to remove mobile devices after thirty days of inactivity, at which time the mobile device is removed from the email server. The device is also hidden from the MDM software so that it is no longer counted for licensing purposes.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.11	Technology Services should perform periodic access reviews for the MDM software and disable inactive accounts after a specified period of inactivity.	Technology Services has turned on software rules that disable inactive accounts, which are triggered by thirty days of inactivity.	**Implemented**
1.12	Technology Services should update the Computer User Request Form on the Denver.One.Team web portal (DOT) to include suspending wireless service when employees leave the City. Periodic reviews should be conducted at least monthly to ensure that wireless plans are not paid for former employees.	Technology Services has updated the Computer User Request Form on the Denver.One.Team web portal (DOT) to include suspending employees' wireless service when they have separated from the City. Termination reports are reviewed weekly by Technology Services to ensure that wireless plans are not being paid for former employees.	**Implemented**
1.13	Technology Services should prevent employees from having both a City-owned device and a stipend by reviewing existing Financial Options Forms prior to granting an employee a new financial option for mobile device usage. Further, Technology Services should direct agency liaisons to perform monthly monitoring to ensure that employees are not receiving dual payments.	Technology Services has implemented procedures that prohibit employees from receiving a mobile device stipend and a City-issued mobile device at the same time.	**Implemented**
1.14	Technology Services should improve training for agency liaisons to ensure that wireless payment monitoring is performed at least monthly to include a review of wireless payments for accuracy and low usage.	Technology Services has improved training for agency liaisons, which includes wireless payment monitoring and periodic reviews for accuracy and low usage.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.15	Technology Services should evaluate all MDM software features and implement those that help enforce City information security requirements. Additionally, Technology Services should provide training to MDM administrators to improve the use and effectiveness of MDM software.	Technology Services has evaluated the MDM application controls and determined that the risks do not justify enabling controls that help enforce City Information Security requirements, such as enabling passcodes, locking a device after inactivity, and the auto-wipe feature. As a result of the assessment, TS did not implement the MDM software security controls to ensure that the City's sensitive and regulatory data is protected. Technology services did provide MDM administrators with training on the MDM software features and functionality.	**Implemented**

Conclusion

For our follow-up work, we performed the following procedures to validate the auditee's response:

- Interviewed key personnel to gain an understanding of the revisions to the Mobile Device Management (MDM) process
- Reviewed the mobile device risk assessment to determine whether key risks were identified and whether controls were evaluated
- Inspected training materials provided by telecom advisory firm Manage Mobility to the Agency Liaisons to determine whether they cover key processes, such as ordering, activating, and dis-connecting devices
- Reviewed the process document for loss or theft of equipment and generated an incident report for devices listed as lost or stolen from Jan 2016 to May 2016; inspected incident tickets to determine whether data was remotely wiped from the devices
- Compared termination reports to mobile device carrier inventory reports to determine whether former employees were removed from wireless service
- Compared stipend reports to mobile device inventory listings to determine whether any employees received a stipend and a City issued mobile device simultaneously

Although the Technology Services department has implemented some recommendations made in the Mobile Devices audit report, others have yet to be acted upon or fully implemented. Despite these efforts, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. Technology Services' decision to move to a different mobile device application has delayed the creation of a Mobile Device Policy, as well as the Acceptable Use forms that would have outlined the City's privacy principals. Due to the restructure of the Mobile Device Policy, the removal of regulated and sensitive data from employee's devices was not addressed. Former employees with access to sensitive or regulated information may retain this information on their personal devices subsequent to their separation from the City. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure that appropriate corrective action is taken.

On behalf of the citizens of the City and County of Denver, we thank staff and leadership from the Technology Services for their cooperation during our follow-up effort and their dedicated public service.