Minneapolis
City of Lakes

Personal/Work-Issued Mobile Devices Policies and Controls Audit

City of Minneapolis

Internal Audit Department

December 6, 2021

Table of Contents

Executive Summary

As part of our rolling audit plan approved by the Audit Committee, the City of Minneapolis (the "City") Internal Audit department conducted an audit of the use of mobile devices (i.e., cell phones and tablets) at the City. The objective of this audit was to review the City's policies and controls related to the use of personal/work-issued mobile devices.

Mobile devices are important IT assets used for a variety of essential tasks and duties for employees to complete their work, and there should be strong governance and oversight in place to ensure the City and government data are protected when employees use mobile devices. Clear expectations and documented processes in place can ensure that resources are being used efficiently and effectively.

The audit scope and approach, testing results, and conclusion are discussed below, followed by a description of the City's mobile device processes in the background section and a detailed description of observations and management's action plans in the final section.

Audit Scope and Approach

The scope of this engagement covered policies and procedures in place and device activity during the period from January 1, 2019 through August 31, 2021, and included:

- Reviewing department and City-wide policies in place related to the use of mobile devices to ensure they are current and sufficient to provide adequate guidance and oversight;
- Assessing the processes for the approval and handling of mobile devices, including billings, and reimbursements, from the application and issuance to disposal, across the City to ensure they are fair, consistent, and adequately documented;
- Verifying the number of department-issued mobile devices across the City, including inactive devices, and the availability of complete and current data related to their use and costs; and
- Assessing controls and processes in place related to data security and the use of government data, to ensure they are adequate and in alignment with best practices.

Results

As a result of this audit, five audit issues were identified:

1. Policies and procedures are not current and sufficient to ensure proper issuance, use and oversight of mobile devices, and are not consistent across the City (HIGH)
2. There is no independent inventory of mobile devices across the City that is accurate, up to date, and able to be reconciled with billing data (HIGH)

3. The guidelines and expectations for what happens to a device no longer needed or used are not consistent across the City (MOD)
4. There is not specific governance language and practices regarding data that may be created or maintained on mobile devices in policies and practices across the City (HIGH)
5. There is no enterprise-wide mobile device management solution in place that covers all mobile devices issued by the City, and there is varying security coverage in place (MOD)

There are many areas of risk to consider, including financial, operational, compliance, and reputation, when determining the relative risk rating. Table 1 below contains the overall evaluation of the severity of the risk and the potential impact on operations. Issues are rated as High, Moderate, or Low.

Table 1.

Personal/Work-Issued Mobile Devices Policies and Controls Audit Observations and Issue Ratings		
High	**Moderate**	**Low**
1. Policies and procedures are not current and sufficient to ensure proper issuance, use and oversight of mobile devices, and are not consistent across the City.		
2. There is no independent inventory of mobile devices across the City that is accurate, up to date, and able to be reconciled with billing data.		
	3. The guidelines and expectations for what happens to a device no longer needed or used are not consistent across the City.	
4. There is not specific governance language and practices regarding data that may be created or maintained on mobile devices in policies and practices across the City.		
	5. There is no enterprise-wide mobile device management solution in place that covers all mobile devices issued by the City, and there is varying security coverage in place.	

- **High Risk:** Some key controls do not exist or are not effective resulting in impaired control environment; high risk improvement opportunities require immediate corrective action
- **Moderate Risk:** Adequate control environment in most areas; moderate risk improvement opportunities identified which require corrective action
- **Low Risk**: Satisfactory overall control environment; small number of lower risk improvement opportunities identified which do not require a management action plan

The details of these observations are included within the *Observations and Management's Action Plan* section of this report, beginning on page 8.

Conclusion

Overall, the City's policies and controls related to the use of personal/work-issued mobile devices need strengthening to ensure consistent, effective, and fair processes. Policies help ensure sufficient oversight is in place for devices and their use. Audit noted some control deficiencies and opportunities for improved governance.

Internal Audit would like to thank Information Technology (IT), the City Clerk's Office, Finance and Property Services, Radio Shop, Minneapolis Police Department, Convention Center for their cooperation and time during this engagement. Audit would also like to thank all the City departments that provided us with mobile device data and information.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Team for this Engagement

Ryan Patrick, CIA, Director of Internal Audit
Huguette Essoh Latte, CIA, Internal Audit Manager
Comlan Alede, Internal Auditor
Travis Kamm, Internal Auditor

IT Primary Contacts

Paul Cameron, CIO
Robert Arko, Deputy Director, IT
Abdeslam Mazouz, CISO
Gina Filigenzi, Director, Service Desk

City Clerk Primary Contacts

Christian Rummelhoff, Director, Records and Information Management
Jessica Velie, City Records Manager

Finance & Property Services Primary Contacts

Dushani Dye, CFO
Lori Johnson, Deputy CFO
Barbara O'Brien, Director, Property Services
Rodney Olson, Manager, Radio, Comm and Electronics

Office of Internal Audit

Phone: (612) 673-5938
Email: InternalAuditDepartment@minneapolismn.gov
Website: http://www.ci.minneapolis.mn.us/audit

Background

Employees use mobile devices across the City for a variety of tasks as part of their work duties. Cell phones and tablets are the most common, but devices may include equipment to access mobile networks, such as MiFi cards, or specialized equipment such as ticket writers.

There are currently three departments that administer mobile devices to employees. The Minneapolis Police Department (MPD) and Convention Center handle their own mobile device processes; IT is responsible for all other departments. The Radio Shop, a division of Finance and Property Services, handled mobile device administration for many City departments until October 15, 2021. Those duties were then transferred over to IT**;** however, the Radio Shop process was active during the audit scope period.

Prior to the transfer of duties, City departments other than MPD and the Convention Center could get devices from the Radio Shop or IT. Management typically decided to acquire a device and set the processes for the departments. Employees could get some mobile devices from either the Radio Shop or IT, but iPads came from IT and some specialized communication equipment from the Radio Shop.

The City utilizes two government-wide mobile device contracts. A State of Minnesota contract and a Federal General Services Administration contract that cover the main wireless providers: Verizon, AT&T, Sprint, T-Mobile, and FirstNet. These provide terms and standard rates governments pay for mobile device services and devices. However, there are many different types of plans and data services the City can choose from the contracts. Typically, Audit observed monthly wireless plan charges per line ranging from $34.99 to $44.99 for phones and tablets, not including the cost of a device, which was often discounted.

Bills are sent to the departments, which work with accounting and finance staff to pay them through the typical City Procurement invoicing process. Devices are paid out of budget line items dedicated for the devices and wireless services.

Below, the mobile device processes across the City are briefly described. The mobile device-issuing departments generally order and administer devices, with receiving departments involved in the handling and

use of devices. Further discussion of parts of the processes is included in the observations below, including inventory management and device disposals.

IT and Former Radio Shop Processes

Departments and management typically determine whether a device is needed and what device to get. The employee or someone in the department, if choosing to go through IT, can order through the online CityLife portal, similar to other work equipment. The selection of available devices depends on what the service providers have; employees can also submit a request for different devices. Managers or other designated approvers sign off on the request, and a device is sent to the employee's place of work or IT and then picked up by an employee. Employees can request help from IT in setting up the device.

The former Radio Shop ordering process had requests sent to the Radio Shop and employees in the Radio Shop facilitated the ordering of devices using the service provider's online ordering page. If the Radio Shop had available used devices on hand, they were reused. Once devices were received, the Radio Shop could help with setting up devices and other services, or an employee could reach out to IT for assistance.

MPD and Convention Center Processes

In MPD and the Convention Center, management determines the need for devices. For sworn MPD officers, a phone is required as part of their equipment and given out when they receive their uniform and duty equipment. Civilian staff in the department can reach out to the Business Technology Unit, which handles mobile device administration, and there is a central staff person in the Convention Center employees can contact to request a mobile device.

Devices are ordered online from the service provider and usually shipped to the employee's work location. MPD officers exclusively use iPhones as part of their equipment; Convention Center employees order the lowest cost device unless an employee wants a specific device and will pay the cost difference.

Mobile Device Data

There are thousands of mobile devices across the City. Due to the observations in Issue 2 below on capturing an exact inventory of devices, Audit summarized invoiced amounts for each department over a period of 6 months, from February 2021 through July 2021, below in Table 2.

Table 2.

Six Months Telephone and Data Charges

MONTHS	RADIO SHOP & IT	CONVENTION CENTER	POLICE		Total
	Verizon Phone/Data	CellCo Phone	First Net Data	Verizon Phone	
February, 2021	$40,627.36	$1,542.88	$41,244.63	$12,292.10	$95,706.97
March, 2021	$33,072.82	$1,614.52	$41,271.70	$12,599.95	$88,558.99
April, 2021	$32,284.55	$1,540.61	$41,262.10	$12,390.19	$87,477.45
May, 2021	$32,936.34	$1,568.34	$39,866.41	$12,689.92	$87,061.01
June, 2021	$49,879.84	$1,568.34	$36,361.12	$12,355.79	$100,165.09
July, 2021	$49,764.17	$1,894.85	$35,014.11	$12,354.47	$99,027.60
Total	$238,565.08	$9,729.54	$235,020.07	$74,682.42	$557,997.11

Observations and Management Action Plans

ISSUE #1. Policies and Procedures

Policies and procedures are not current and sufficient to ensure proper issuance, use and oversight of mobile devices, and are not consistent across the City. *(HIGH)*

Observation

Audit found the City-wide cell phone policy was last updated in 2001 and does not reflect current practices or capabilities of cell phones; in addition, it was limited to cell phones in the scope.

The City-wide policy gives the responsibility of oversight and management of cell phones to individual departments, and Audit observed that a handful of departments have created their own policies to supplement the City's. Most departments have not. In the department policies, dates of last updates and details vary, however, Audit noted that:

- Handling procedures and expectations are not consistent across the City
- The application and approval process for mobile devices is not clearly and consistently documented
- Some processes are not specifically covered in the policy and procedure documents, and the documents are not sufficient to ensure proper issuance, use, and oversight of mobile devices
- Mobile device guidelines and expectations are not readily available to most City employees.

Criteria

Policy and procedure documents should grow and adapt with an organization, and it is best practice to review and update them, if necessary, on at least an annual basis. The review should not happen only when there are actual changes to the policy and procedure documents but should be a regular activity to ensure that changes (if any) are incorporated in a timely manner. The policies and procedures should be consistent across the enterprise, or deviances approved and documented.

It is best practice to formalize and standardize key processes to strengthen the control environment, improve efficiencies, and mitigate the risk of non-compliance. Documenting processes helps reduce operational

ambiguity by providing consistency in operations and making monitoring easier. It also allows for stakeholders to be informed and take action to reduce risks.

Cause

As the use case and capabilities of mobile devices have expanded in recent years, City policies and practices have not evolved to reflect the increased importance and risks associated with mobile devices.
Public Works is listed as the administering department of the current City-wide cell phone policy, rather than IT. With the decentralized practices of mobile devices at the City, with multiple departments issuing devices, IT has not centralized or asserted control over mobile devices.

Risk

Outdated and insufficient policy and procedure documents increase the risk of non-compliance and decrease the usefulness of the documents. Users may develop workarounds or their own processes, leading to inconsistencies across the enterprise, and increasing the risk of improper handling, differing expectations, and a lack of oversight and monitoring of mobile devices.

Recommendation

Internal Audit recommends that IT management:

- Update the City-wide cell phone policy to include all applicable mobile devices and reflect the governance structure and mobile device standards management decided upon.
- Establish procedure documents that reflect current practices, and cover all parts of the mobile device lifespan, including application and approvals, handling and use, oversight and disposals. Approvals and requirements for obtaining mobile devices should be documented and based on identified business needs and the working environment.
- Establish a process to review policies and procedures at least annually, with changes tracked in a track log, to ensure documents stay current. Communicate changes and updates to department IT liaisons and City employees on a regular basis, and work with the Convention Center and MPD, the other device-issuing departments to recommend policies and best practices concerning mobile devices
- Create a process to ensure that departments supplemental policy or procedure documents, if allowed, are documented, and do not conflict with standards set by IT.
- Work with City Leadership and departments on centralizing and clarifying mobile device management roles and responsibilities and policymaking.

Management Action Plan

The IT Department has been working on a governing policy for mobile devices for several months. Our goal is to publish this policy in Q1 2022. The goal of this policy is to set rules and best practices around the lifecycle, use, and managing mobile devices to access City resources and data.

For the devices IT manages we will create and update procedure documents covering mobile devices including lifespan, applications, approvals, handling and use, oversight, and disposals. This will happen in concert with implementing the inventory management system and the mobile device management, both of which will be needed to fully implement the procedures.

IT will start a discussion with City leadership to explore the possibility of mobile device consolidation in IT.

Target remediation date: 12/1/2022
Responsible party: Abdeslam Mazouz

ISSUE #2. Mobile Device Inventory Management

There is not an independent inventory of mobile devices across the City that is accurate, up to date, and able to be reconciled with billing data. *(HIGH)*

Observation

Audit observed that the majority of the City departments do not maintain mobile devices inventory separate from their service providers. However, most departments have no separate, complete, and up-to-date inventory to manage to identify all assigned devices, individual users, departments' common use devices, and the plan's cost selected for each line. Some departments have also developed inventory processes, but it is not practiced across the whole enterprise.

Many departments rely on their services providers' databases to pull information related to their devices, users' names, and paid plans. As a result, an aggregate inventory reconciliation by Audit could not be completed for mobile devices across the City. Cell phones and tablets are not assigned asset tags or other identifying physical features. Some mobile device issuing departments have used features such as the SIM card number or MIN numbers to track devices.

As part of the City procurement invoice payment process, each department checks the items or services charged on their invoices, approves, and sends them with a coding string for payment. Audit observed that multiple mobile devices for a department may be listed under one employee's name in the service invoices who is not the primary user. Some devices are not listed with an identifying name. Audit also noted occurrences of devices being assigned to users who have separated from the City. Departments rely on this billing data for their primary mobile device inventory, and it is not up to date. This further complicated an independent reconciliation of mobile devices. In addition, if a device does not have an attached data plan, such as iPads, those devices may not appear on the billing invoices which is currently the primary inventory system in place.

Criteria

Mobile devices are City assets, and it is important that they are tracked throughout their lifecycle. It is best practice to implement an inventory management system to trace the complete lifecycle of an asset, from when an organization purchases it until its disposal. Each asset should have a unique identification and an owner who maintains it. Regular independent reconciliations should occur and be documented, and the data kept current and up to date.

Cause
The mobile device process at the City is decentralized, with much of the oversight responsibilities given to individual departments and a lack of central oversight of the process. There is no established mobile device inventory management system at the City; departments rely on their service providers' database to pull their inventory list. There is no separate inventory list at each department to reconcile with services providers' invoices.

Risk
A lack of an independent mobile devices inventory management across the City increases the risk of duplicating purchases, theft, unawareness of loss, and could lead to overpaying for mobile devices services and non-compliance with regulations. City assets may be lost or misused without management knowledge if there is not proper oversight built into the mobile device process and clear expectations on how mobile devices should be managed.

Recommendation
Internal Audit recommends IT management work with department IT liaisons to create an independent mobile device inventory process for departments, such as a spreadsheet that may contain information such as the type of mobile device, the user, device identification, and other relevant information. IT liaisons or other identified parties in departments should be given training and guidance from IT on managing devices. A regular documented reconciliation of mobile devices should occur.

IT management should also identify and establish ways to physically track devices similar to other IT equipment, such as through asset tags on devices. This may be part of a mobile device management solution. There are opportunities to implement a mobile device inventory management system to ensure their availability and monitor their lifecycle costs.

Internal Audit recommends IT management work with City Leadership and departments on centralizing and clarifying mobile device management roles and responsibilities and policymaking.

Management Action Plan

The IT Department roadmap for 2022 addresses the need for robust hardware asset management (including management of mobile devices) through the purchase, configuration, and implementation of ServiceNow ITAM (IT Asset Management.) This solution will allow for the management of all assets, including mobile devices, within an enterprise platform, providing a single source of truth for both hardware and software, replacing the many disjointed and manual processes and tools that aim to do this today.

ServiceNow ITAM will position us to successfully meet both the strategic and operational requirements of asset management deemed critical for the City, including but not limited to:

- Optimizing inventory to improve asset utilization and service delivery
- Sourcing and transferring assets by location
- Supporting real-time monitoring of compliance
- Ensuring accuracy with regularly scheduled audits

- Planning and executing device lifecycles with refresh and retirement of assets

Acquiring ServiceNow ITAM will require an investment of $89k annually.

The initial focus of the ITAM implementation will be devices that access City data or the City network. This would include mobile devices. It should be noted that the City is still exposed to risk as IT Services is not currently responsible for all assets.

The IT department did receive a position as part of the mobile device consolidation with the Radio Shop. We will be utilizing this position to help manage the asset inventory.

IT will start a discussion with City leadership to explore the possibility of mobile device consolidation in IT.

Target remediation date: 9/30/2022
Responsible party: Dana Nybo

ISSUE #3. Mobile Device Disposal

The guidelines and expectations for what happens to a device no longer needed or used are not consistent across the City. *(MOD)*

Observation

Mobile device-originating departments follow different processes and expectations when it comes to returning mobile devices, such as when a device upgrade occurs or an employee separates from the City. Specifically:

- For devices issued by IT, devices are viewed as the property and responsibility of the department that purchased the device, and there is not an expectation that devices are returned. The purchasing department can decide whether to keep the devices, reuse them, or recycle them.
- For devices issued by the Radio Shop, there is an expectation that devices are returned to the Radio Shop, and they may be reused. If an employee separates, the return process is not fully incorporated into City's separation process. However, as of October 15, 2021, control of Radio Shop-issued devices was transferred to IT.
- For MPD, there is an expectation that mobile devices are returned, and devices are considered similar to a piece of other department-issued equipment that is collected when an employee departs. The Business Technology Unit is responsible for managing devices, and devices may be recycled or reused.
- For the Convention Center, there is an expectation that devices are returned as part of the employee separation process. However, if employees contributed to part of the cost of mobile devices, those devices are not required to be returned.

The departments above have options for recycling devices; MPD may be able to recover some of the costs of their devices when recycled. Devices returned to IT can be electronically wiped of data, or IT will provide instruction for departments on how to reset a device, but that process is also not required and consistently done for all devices.

Criteria
Mobile devices, including cell phones and tablets, are City-owned devices, and should be treated similar to other IT equipment, such as laptops. The City incurs costs for their purchase and continued use. When an employee separates, access should be restricted to all systems and devices, and equipment gathered should be cleaned and either reused or recycled in accordance with established and documented practices.

Cause
The City's mobile device process is decentralized, with several parties responsible for issuing mobile devices; those parties have differing expectations pertaining to the responsibility and control of mobile devices. In current policy and practices adapted over time, the management and oversight of mobile devices are generally deferred to the department that purchases the devices and/or plans, rather than a central function such as IT.

Risk
Mobile devices may still have a residual value to the City after use by the original user, creating financial risks to the City when a device is not returned or is disposed of when it may be sold or reused. Inconsistent practices and expectations of what department controls a device or is responsible for it create the risk of unfairness to City employees as well as unclear oversight and management duties. Devices may contain government or confidential data, and a lack of a consistent process for wiping data and disposing of devices increases the risk of data breaches and loss of government data.

Recommendation
Internal Audit recommends IT management centralize and standardize the disposal process of mobile devices. Specifically:

- Policies should be updated and communicated, establishing clear ownership expectations of City-issued mobile devices.
- The separation process for all departments should include the collection and deactivation of mobile devices.
- There should be clear and documented standards for whether devices may be reused and assigned to a different employee or recycled.
- All mobile devices no longer used should be cleared of data and factory reset.
- All returned or disposed of devices should be treated and recycled in the same manner across the City with the outcome of a device documented.

Management Action Plan

The IT Department has been working on a governing policy for mobile devices for several months that will address the final disposition of mobile devices. Our goal is to publish this policy in Q1 2022 to provide better clarity around ownership expectations and how devices may be reused. Using this policy as well as the implementation of the inventory management system outlined in Issue 2 will assist us in establishing processes related to device disposal throughout the remainder of 2022. The goal of these processes will be target the following areas:

- Collection, deactivation, and factory reset of all mobile devices issued by the IT department.
- Devices will be either reused if possible or recycled/donated in an appropriate manner.

Target remediation date: 12/1/2022
Responsible party: Gina Filigenzi

ISSUE #4. Data Governance

There is not specific governance language and practices regarding data that may be created or maintained on mobile devices in policies and practices across the City. *(HIGH)*

Observation

Audit observed that there is not specific governance language and practices regarding data that may be created or maintained on mobile devices in policies and practices across the City. There is a lack of language in coverage in the City's current cell phone policy pertaining to government data, and the current cell phone policy is not sufficient in providing adequate guidance.

Enterprise-wide information policies may cover mobile devices implicitly if they are platform agnostic, for example such as the Records Management Policy or Privacy Principles. In general, considerations in government data and mobile devices are not clear for employees, and by default, employees are allowed to work on personal devices or do personal business on city issued devices without careful thought to the potential impact and consequences. As a result, there is a lack of documented controls in place.

In addition, Audit noted opportunities for the data request workflow to specifically incorporate mobile devices in all aspects of the process and ensure responsive data is included. The current process and system used to extract data from mobile devices is time consuming and inefficient, requiring a device to be physically presented and examined.

Criteria

City policies and procedures should reflect the realities of employees' work environment. Mobile devices may require unique considerations in data governance practices and conversations, and it should be clear to all City employees and users of government data what the expectations and guidelines are when using mobile devices for government work.

When fulfilling data requests, it is important that all responsive data be located and available for review; if the City continues to adopt more flexible working arrangements, more data may be on mobile devices, requiring that methods to extract data be quick and comprehensive to ensure timely responses.

Cause

As the capabilities of mobile devices have evolved over the years, policies at the City have not been updated to reflect the increased use and functions of mobile devices. Information governance policies were created platform agnostic or without considering the unique situations mobile devices presented. In addition, there is increased importance in mobile device governance with the shift to remote work due to COVID-19.

Risk

insufficient policy and procedure documents increase the risk of non-compliance. Users may develop workarounds or their own processes, leading to inconsistencies across the enterprise, increasing the risk of

improper handling, differing expectations, and a lack of data oversight. Data may be improperly accessed or lost, resulting in data breaches. Data may also be improperly or unknowingly stored, creating difficulties in responding to data requests.

Recommendation

Internal Audit recommends that City Clerk management continue to conduct a review of information governance policies that may involve mobile devices and update them to provide clear guidelines for employees. Procedures should be updated or created to reflect current practices; controls should be identified and documented as part of this process. A part of this review may involve considerations of personal devices and other situations, and management should work with IT and other applicable parties to make determinations. These changes should be communicated to City employess.

Management should continue to explore options for data requests, including working with IT to identify software that may allow for more efficient and effective extraction of data requests. In addition, the data request process, which is part of a workflow system, should be reviewed and revised to ensure mobile device data is formally included in templates and workflow documentation.

Management Action Plan

Management agrees with the findings and appreciates the thoughtful approach to the audit.

Policy Framework - The City Clerk, the Chief Information Officer, City Attorney, and others collaborate to maintain City information policies that address the creation, receipt, management, storage, access, protection, use, and disposition of information. These policies set goals, identify roles and responsibilities, and establish policy controls. Generally, controls are platform agnostic controls, reflecting the varied operations of twenty-two City departments and the different technologies in use. However, as the Audit findings indicate, mobile devices present unique challenges that should be explicitly addressed.

To address these findings, management will take the following actions:

- Enact a Mobile Device Policy establishing controls unique to mobile devices and providing guidance on the implementation of existing controls on mobile devices. A key new policy control will require City business to be conducted on City-managed devices.
- Publish enterprise training resources covering records management on mobile devices.
- As other information-related policies are updated, ensure they are in accord with the Mobile Device Policy.

Data Practices Workflow – State law requires the City to respond to requests from the public for City data. Clerk's staff works with departmental data holders to locate and gather requested data, evaluate its classification, and remove or redact protected data. Each step is more challenging when responsive data resides on a mobile device, for example, data holders must manually search for and copy responsive text messages.

To address these findings, the City has already acquired software to facilitate searching and collecting text message data to enhance the manual process. Additional actions we've outlined for implementation in 2022:

- Acquire and deploy software to manage those mobile devices most likely to be involved in data requests or contain records.
- Revise the data practices workflows to reflect the new policy controls and collection capabilities related to mobile devices.
- Include guidance about data requests involving mobile devices in the enterprise training resources mentioned above.

Target remediation date: July 1, 2022
Responsible party: Christian Rummelhoff

ISSUE #5. Mobile Device Management

There is not an enterprise-wide mobile device management solution in place that covers all mobile devices issued by the City, and there is varying security coverage in place. *(HIGH)*

Observation
Audit observed that there is not an enterprise-wide mobile device management solution in place that covers all mobile devices issued by the City, and there is varying security coverage in place. iPads, issued by IT, have a function called AirWatch but not cellular devices. Some devices have other systems, and phones have some portioned-off sections that can be wiped; however there is no consistency and the capabilities are limited.

The Minneapolis Police Department utilizes AirWatch for all of its devices; however, devices issued by the Radio Shop rely on the IT process and coverage, and as a result, there is not equivalent to a mobile device management solution that can assist with functions such as monitoring, security, and separation and preservation of government data, among other functions.

Criteria
Mobile devices are City assets and important tools employees use to access City work tools and services to fulfill their work duties, and City assets should be adequately protected. Government data and user access on those devices should be sufficiently protected through security and oversight capabilities on all mobile devices issued by the City, and if personal devices are allowed for government work, on personal devices as well.

Cause
The City's mobile device process is decentralized, with several parties responsible for issuing mobile devices, and the management and oversight of those devices generally deferred to the department that purchases the devices and/or plans, rather than a function such as IT. As the use cases and capabilities of mobile devices have expanded in recent years, City policies and practices have not evolved to reflect the increased importance and risks associated with mobile devices.

Risk
Mobile devicesare City assets and are used to access important City tools, such as Outlook and internal applications. There is a risk that devices may be lost, stolen, or inappropriately accessed without proper

protections in place to limit the impact. In addition, without proper separation between City data and personal data, there may be violations of data practices and best practices.

Recommendation
Internal Audit recommends IT management continue to explore mobile devive management solutions, and implement a solution on all City-issued mobile devices, including tablets, as soon as feasible. Older devices or systems should be upgraded as needed to ensure there is universal coverage.

In addition to working with the Convention Center and MPD, IT should also work with individual departments on the implementation, training department liaisons and updating policies and practices to ensure the mobile device management system covers all devices. Roles in IT should be updated or created to handle mobile device oversight.

In conjunction with policy and data practices discussions, if employees are allowed to use personal devices for work purposes, IT management should include those devices in the mobile device management solution.

Management Action Plan

The IT Department started a pilot for a Mobile Device Management (MDM) program earlier this year. We are leveraging Microsoft Intune to manage City issued devices. We have requested funding for a full-time employee (FTE) through the budget process to continue this initiative. The MDM budget request is included in the Mayor's recommended budget but only includes one-time support for 2022. There will be a need for additional ongoing support for maintaining the MDM program.

Personal devices will not be allowed to directly access the internal City network and will not be included in the MDM solution.

Devices managed by other departments will also not be included in the MDM solution.

Target remediation date: 12/1/2022
Responsible party: Abdeslam Mazouz