



CITY AUDITOR'S OFFICE

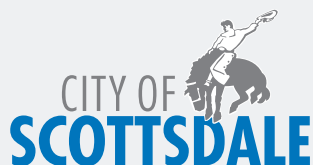
Asset Management of Mobile Computing Devices

October 12, 2026

AUDIT NO. 2605

CITY COUNCIL

Mayor Lisa Borowsky
Barry Graham
Jan Dubauskas
Adam Kwasman
Kathy Littlefield
Vice Mayor Maryann McAllen
Solange Whitehead



WHY WE DID THIS AUDIT

An audit of Asset Management of Mobile Computing Devices was conducted pursuant to the City Council-approved fiscal year (FY) 2025/26 Audit Plan. The objective of the audit was to evaluate the effectiveness of controls and management of mobile computing devices throughout their asset lifecycle. For the purpose of this audit, mobile computing devices include laptops, tablets and smartphones.

BACKGROUND

The Information Technology (IT) Department supports the City's operations by managing infrastructure, network operations, security policies, and end-user devices. As part of these responsibilities, the department manages the asset lifecycle for mobile computing devices. This includes device acquisition, setup, configuration, security management, technical support, and final asset disposition.

Additionally, the department administers the related voice and data service plans for these devices. Annual expenditures for voice and data services averaged about \$1.4 million over the past four fiscal years.

AUDIT HIGHLIGHTS

October 2026

Asset Management of Mobile Computing Devices

Audit No. 2605

WHAT WE FOUND

Stronger receiving and disposition controls are needed to ensure accountability and safeguard mobile computing assets.

Specifically,

- Receipt of smartphone and tablet purchases need to be independently verified, recorded, and securely stored; smartphones are not labeled or barcoded.
- Disposition procedures and documentation are insufficient to ensure accountability.

Mobile devices are managed across multiple systems, creating inefficiencies and inconsistent processes.

- Decentralized inventory records contributed to inconsistent data, challenges in tracking devices and service requests, and difficulties monitoring compliance with security requirements.
- Consolidating mobile device records could streamline processes and improve the accuracy and reliability of asset information.

About 4% of mobile phone service lines were associated with terminated employees, and information for reviews of other device charges is insufficient.

- Employee changes are not always communicated timely, and monthly service charges are not adequately validated.
- Monthly cellular service charges, totaling approximately \$1.4 million annually, are generally reviewed for reasonableness. Device information on billings contained incomplete or inaccurate information, making validation difficult.
- Carrier services purchased through cooperative agreements were not approved by the Purchasing department.

Review of technical and security controls identified several high or critical priority areas.

The technical review conducted by our IT audit consultant, Protiviti, identified several high or critical priority issues related to conditional access, device configuration, and vulnerability management. A separate comprehensive report of their recommendations was provided to the IT department.

WHAT WE RECOMMEND

We recommend the Information Technology Department:

- Evaluate its receiving and disposition procedures to ensure adequate separation of duties and accountability of assets.
- Explore consolidating mobile device records, review its asset records to improve data reliability and effectiveness of monitoring activities.
- Improve employee off-boarding procedures, verify monthly service carrier charges, and obtain required Purchasing department approvals.
- Address technical recommendations from the IT audit consultant.

The IT department agreed with the recommendations and estimates implementation by October 2027.



October 12, 2026

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Asset Management of Mobile Computing Devices*, which was included on the Council-approved FY 2025/26 Audit Plan. This audit was conducted to evaluate the effectiveness of controls and management of mobile computing devices throughout their asset lifecycle.

The audit evaluated the City's management of mobile computing devices, including laptops, tablets, and smartphones, and found that controls over receiving, inventory tracking, and asset disposition should be strengthened to improve accountability and safeguard City assets. The audit also identified inefficiencies caused by maintaining mobile device records across multiple systems. This contributed to inconsistent data, challenges in tracking devices and service requests, and difficulties monitoring compliance with security requirements.

For the related voice and data services, our review found that processes for communicating changes in employee status or device assignment and reviewing monthly charges could be improved to minimize potential overpayment of unnecessary services. Review of the service plans found that approximately 4% of mobile phone lines were associated with terminated employees and there was insufficient information to fully validate some accounts.

The technical review conducted by our IT audit consultant, Protiviti, identified several high or critical priority issues related to conditional access, device configuration, and vulnerability management. Protiviti's comprehensive report, which included security-related findings and observations, was separately provided to the IT department and briefly summarized in this published report.

If you need additional information or have any questions, please contact me at (480) 312-7851.

Sincerely,

Lai Cluff, CIA
Acting City Auditor

Audit Team:

Elizabeth Brandt, CIA – Sr. Auditor

TABLE OF CONTENTS

OBJECTIVE AND SCOPE	2
BACKGROUND	2
Figure 1. Technology Asset Life Cycle.	2
Figure 2. IT Department Organization.	3
Figure 3. Annual voice and data service costs by fiscal year.	4
FINDINGS AND ANALYSIS	5
1. Stronger receiving and disposition controls are needed to ensure accountability and safeguard mobile computing assets.	5
2. Mobile devices are managed across multiple systems and platforms, creating inefficiencies and inconsistent processes.	8
Figure 4. Mobile device processes are managed across multiple systems and platforms.	9
3. About 4% of mobile phone service lines were associated with terminated employees and information for review of other device charges is insufficient.	12
Figure 5. Examples of same-model devices with different data plan costs.	14
4. Review of technical and security controls identified several high or critical priority areas. ...	15
METHODOLOGY	16
MANAGEMENT ACTION PLAN.....	18

OBJECTIVE AND SCOPE

An audit of *Asset Management of Mobile Computing Devices* was conducted pursuant to the City Council-approved fiscal year (FY) 2025/26 Audit Plan. The audit objective was to evaluate the effectiveness of controls and management of mobile computing devices throughout their asset lifecycle.

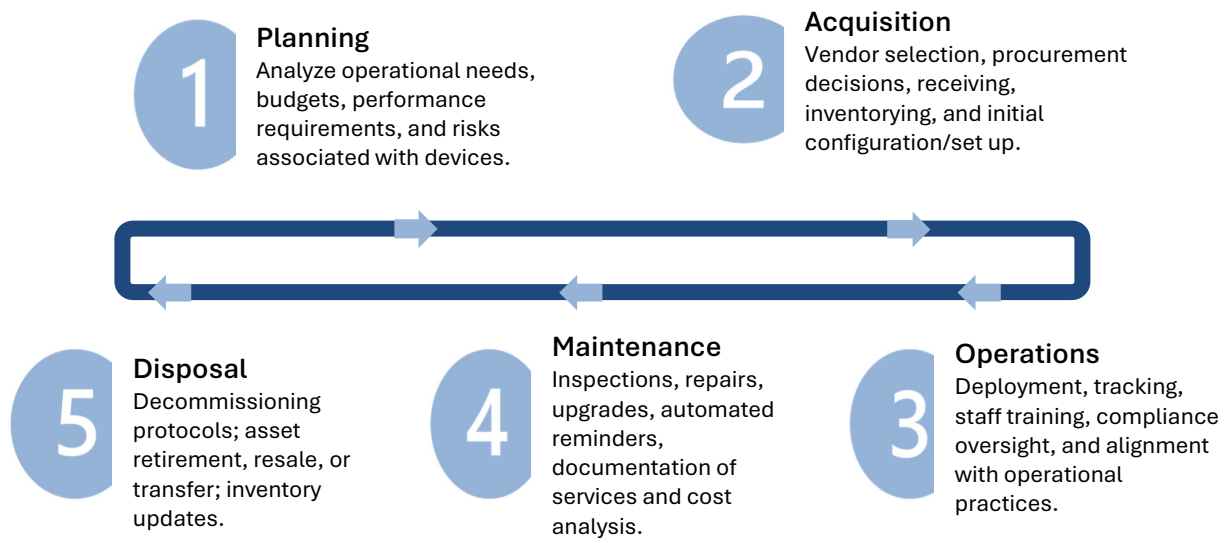
The audit examined the policies, procedures, and controls over purchasing, tracking, disposition, and IT security of laptops, tablets, and smartphones. Additionally, we reviewed management of cellular and data service for these devices. The audit covered asset management of laptops but did not review the overall PC Replacement program, which involves the procurement and routine replacement of end-user computers.

Technical review of security controls and configurations was performed by Protiviti, our IT audit consultant for this engagement. Their detailed findings and conclusions were provided to the IT department for review and remediation. Due to the sensitive nature of security-related findings, only a brief summary of those results is included in this report.

BACKGROUND

The Information Technology (IT) department supports the City's operations by managing infrastructure, network operations, security policies, and end-user devices. As part of these responsibilities, the department manages mobile devices through their entire lifecycle. As illustrated in Figure 1, this includes procurement, inventory, deployment, management, maintenance, and retirement.

Figure 1. Technology Asset Life Cycle.



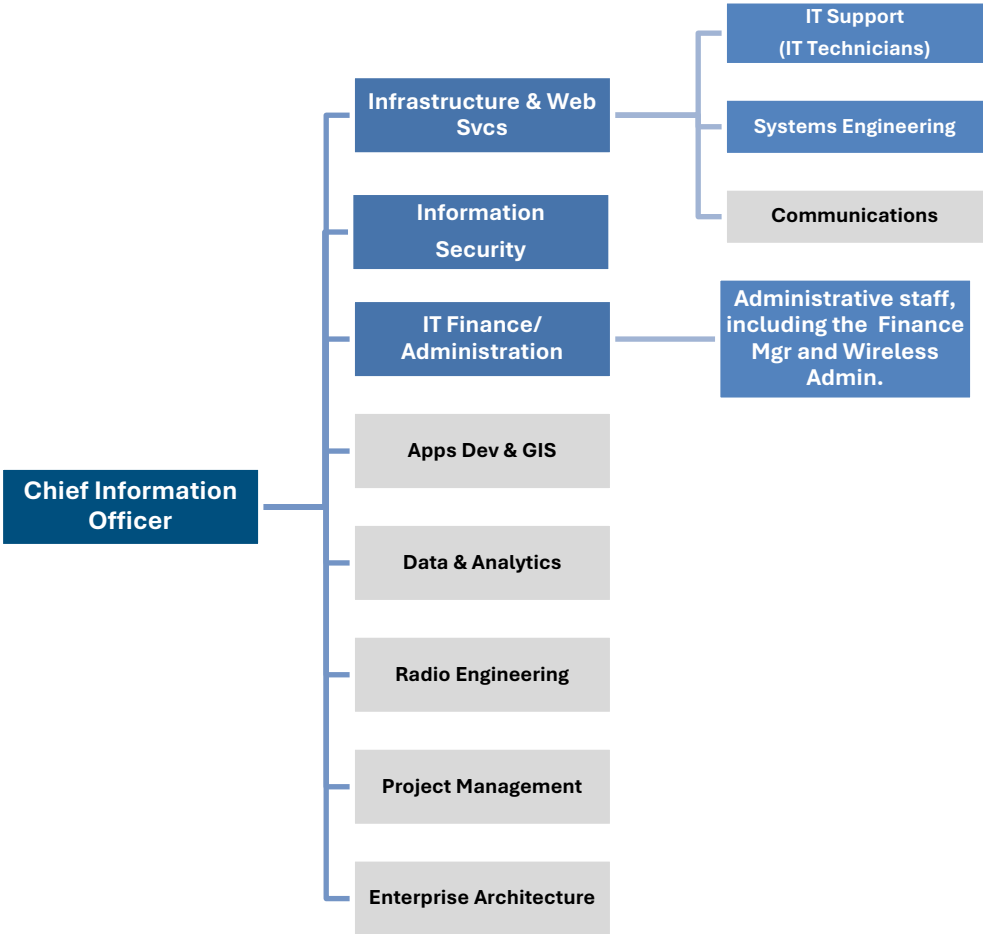
SOURCE: Auditor analysis of industry publications and best practice guidance for asset management.

For the purpose of this audit, mobile computing devices include laptops, tablets and smartphones. As of July 2026, the IT department’s records showed approximately 2,000 laptops, 1,200 mobile phones, and 650 tablets.

Roles and responsibilities for management of mobile devices.

The Information Technology department manages mobile devices through the asset lifecycle, including device setup, configuration, security management, technical support, and final asset disposition. As illustrated by Figure 2, several teams within the IT department play a significant role in managing mobile devices: IT Support, Systems Engineering, Information Security, and IT Finance and Administration.

Figure 2. IT Department Organization.



SOURCE: Auditor analysis of IT department organizational chart and process walk-throughs.

Key Roles and Responsibilities:

- **Planning:** The IT Support and IT Finance teams evaluate operational needs and plans for device acquisition. Laptops follow a scheduled five-year replacement cycle.
- **Acquisition:** IT Finance processes the purchase of approved devices. The central warehouse and IT Finance staff receive laptops, tablets, and smartphones. IT

technicians setup and configure all devices, including applying barcode tags when required and provisioning of devices.

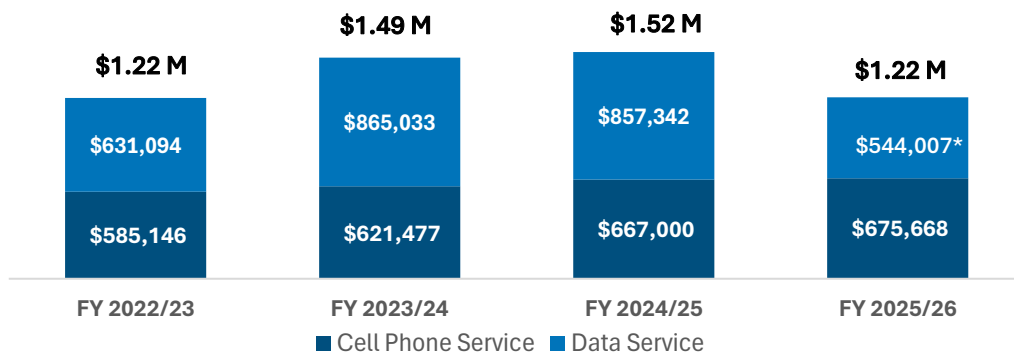
- **Operations:** IT provisioning of mobile devices includes installing necessary software, assigning a device user, applying security configurations, delivering the device to the assigned user, and providing usage training as needed. Once deployed, the IT department continues to manage the device’s access to network resources, as well as applying security and software updates.
- **Maintenance:** The IT Support team performs ongoing device maintenance including tracking repairs, service requests, upgrades, and provisioning of replacement devices. Systems Engineering and IT Security teams oversee compliance with security requirements. IT Finance administers voice and data service plans.
- **Disposal:** Departments report devices that are lost, stolen, no longer needed, or requiring service cancellation. Assigned IT staff purge data, remove barcodes when needed, update inventory records, and determine whether devices should be sold, destroyed, or repurposed based on condition and business need.

Voice and data service for mobile devices

Annual expenditures for voice and data services from cellular providers averaged about \$1.4 million over the past four fiscal years as illustrated by Figure 3. While costs appeared to be trending upwards, total data service charges in FY2025/26 were lower than the prior two fiscal years because the service carrier applied two adjustments totaling approximately \$350,000, which IT staff explained were one-time customer retention credits. These plans are administered by IT Finance team, and monthly costs are allocated to client departments through journal entries. As of August 2026, services included:

- Voice and data for approximately 1,200 mobile phones.
- Data-only service for approximately 1,800 devices, including laptops, tablets, and mobile hot spot devices.

Figure 3. Annual voice and data service costs by fiscal year.



*Based on review of account invoices and information provided by IT staff, FY 2025/26 expenses are lower due to a one-time customer retention credit of approximately \$350,000.

SOURCE: Auditor analysis of general ledger reports from FY 2022/23 to FY 2025/26. Amounts shown include all costs charged to Communications services: Cellular Phones, and invoices paid for the City’s primary cellular data service account.

FINDINGS AND ANALYSIS

1. Stronger receiving and disposition controls are needed to ensure accountability and safeguard mobile computing assets.

Receiving and disposition controls are intended to protect city assets and ensure accurate inventory and record-keeping. For mobile devices, procedures varied based on type of device, and controls need to be strengthened to safeguard city assets. Specifically, receiving procedures for tablets and smartphones lack adequate separation of duties, smartphones are not assigned barcodes, and documentation of dispositions need improvement to ensure accountability. These control weaknesses limit the city's ability to track device custody, reconcile inventory, and verify that dispositions were properly authorized and documented.

A. Receipt of tablets and smartphones purchases need to be independently verified, documented in the financial records, and securely stored until inventory procedures are complete.

With some exceptions, many goods purchased by the City are received, verified, and recorded by the central warehouse. Although purchased laptops are received by the central warehouse, Administrative Regulation provides an exception for tablets and smartphones, allowing these to be delivered directly to the IT department. However, the department's existing procedures do not adequately mitigate the risk of reduced separation of duties.

- **Lack of separation of duties** – For smartphones, the administrative employee who placed the order also received the shipment and recorded the devices in inventory. For tablets, the same employee who placed the order also received the shipment, but an IT technician performed the barcoding and inventory entry. Neither process includes independent confirmation that the items received agree with the order and invoice.
- **Documentation of items received is not recorded in the financial system or required for payment** – Typically, when the central warehouse verifies items and quantities received, this information is recorded in the financial system, and a

copy of the receiving document is uploaded as an attachment. However, items delivered directly to the department may not follow this process.

Because the department has not created a separate requisition for the purchase of equipment, the payment process does not require receiving documentation. This makes it difficult to reconcile the approved order, shipment received, invoice, and asset record to confirm that all equipment ordered was received and inventoried.

With minor exceptions, tablets and smartphones are ordered through the cellular service providers.

- The cellular plans cover basic phone replacement every two years. Departments are charged for model upgrades or replacements earlier than two years.
- Tablets are purchased at contract prices.

- **Devices waiting to be inventoried are not securely stored** – After tablets are received by the administrative employee, they are kept in the employee's cubicle until they are transferred for asset tagging. All IT employees have access to this area. New mobile phones are stored in a locked drawer. In contrast, all other

computers and devices are delivered by the central warehouse to a secured storage room where they are barcoded and added to the asset inventory.

B. Smartphones are not barcoded, and technology asset numbers should be controlled.

Asset barcoding provides a unique identifier that allows each device to be properly accounted for. IT department policy details the types of technology equipment that requires barcoding and the asset numbers are maintained in the IT Service Management System. Among other things, this includes monitors, printers, networking equipment, and all equipment containing a processing chip and running an operating system. However, barcode numbers are not system-generated, and smartphones are not required to have a City asset tag.

- **Barcode numbers should be controlled to ensure that all assets are accounted for in the inventory records** – The IT department generates asset barcodes and adheres them to technology assets for required devices. An internal naming convention identifies the asset make and model, along with a sequential number. However, the numbers are not system-generated; they are generated by the technician based on the internal naming convention. As a result, data entry errors in naming or numbering assets may be made.

- **City-owned smartphones do not have identifying tags or assigned barcode numbers** – City-owned smartphones are not physically labeled with identifying tags or barcode numbers, making them difficult to distinguish from other devices. Although WTS tracks devices by serial number and assigned phone line, serial numbers are not visible on the exterior of the phones. IT policies do not require smartphones to be barcoded. Adding scannable barcode labels would allow staff to identify and verify devices without logging in and to enter asset numbers accurately, reducing data-entry errors during issuance, tracking, and disposition.

Administrative Regulation 227: Non-Capital Assets

- High-Risk non-capital assets must be labeled as “City of Scottsdale Property”.
- Additionally, a physical inventory should be performed and asset records, such as assigned employee, location, and purchase/disposition records, must be maintained.

SOURCE: Auditor summary of AR 227.

C. Disposition procedures and documentation are insufficient to mitigate the risk of missing or stolen devices.

At the end of their useful life, devices are disposed of through surplus auction or destruction; a small number of devices may be kept for spare parts. Tracking and documenting the disposition of assets is essential to ensuring financial accountability and IT security. Existing disposition procedures need to be enhanced to strengthen controls and ensure accountability of city assets.

For tablets and laptops, we found the following procedural weaknesses:

1. **Accurate transfer of custody records needed** – IT Technicians are responsible for updating the status and location of an asset to “Waiting for Surplus” and “Surplus Items in Cage” when an asset is identified for disposition. However, there is no validation that the item was physically dropped off to the surplus cage (the room where items are prepared for disposition and transfer to the warehouse for auction). This status can be updated in the asset management system at any time, and a log

of items dropped off is not required. Additionally, in some instances it appears that the location was not updated; about 2% of assets with surplus-related status still showed other city locations.

2. **Insufficient documentation prevented verification of items transferred to the warehouse and could result in lower cost recovery** – Warehouse employees review and sign off on the items transferred to their custody for surplus auction. However, the Warehouse Surplus Form completed by IT technicians provides counts using general descriptions, such as “desktops” or “monitors”. Because the form does not contain serial numbers, model numbers, or other unique identifiers, and City barcodes are removed prior to transfer, the specific items transferred cannot be verified by the Warehouse.

Furthermore, the lack of information on the device model and condition prevent the Warehouse from effectively advertising the items for auction, potentially resulting in lower bids and reduced cost recovery for the City. Technology equipment is often advertised as “Pallet of Assorted Computer Equipment”.

3. **Final asset status does not accurately reflect disposition methods** – When the surplus technician delivers devices to the warehouse for auction or to a third-party vendor for destruction, devices are updated to “Surplus” status, regardless of the disposition method. Without a separate status to identify assets disposed of through destruction or other method besides surplus auction, Management cannot fully verify that all items were properly disposed.

For smartphones, we identified the following control weaknesses:

1. **Phones identified for disposition are not secured or tracked** - Phones are sent back to the IT Wireless Administrator for disposition. Broken devices are sent to the surplus technician for destruction by the third-party vendor. Other devices remain in custody of the Wireless Administrator. Since March 2026, the department has held to these phones in anticipation of implementing a “buyback” program. However, there is no log of the phones held for buyback, the devices are stored in the employee’s workstation, and there is no asset barcode to identify the devices being held.
2. **Final disposition information is not recorded; inventory records do not provide data on what happened to devices** – For Verizon phones tracked in the WTS application, the Wireless Administrator changes the device status to “Final”, regardless of whether the phone was destroyed or disposed of in some other method. For AT&T phones, a status is not recorded, but the old device model is replaced by a new device. Overall, phone inventory records do not provide information on how many phones were sent for destruction or auction.

D. A replacement policy has not been established for smartphones and tablets.

Although standard model smartphones are eligible for replacement every two years by the cellular provider at no additional cost, City employees do not always choose to do so. While keeping the devices a little longer can reduce staff time spent setting up new phones, the department should evaluate appropriate replacement cycles for phone models in active status. This would help ensure they are still supported by the manufacturer and security features continue to meet city objectives.

Recommendations

The IT department should:

- 1.1 Assess and update internal procedures to ensure adequate separation of duties for the ordering, receiving, and recording of mobile phones and tablets. Procedures should also ensure that purchases of equipment have approved requisitions and receiving documentation prior to invoice payment.
- 1.2 Require secure storage for tablets and smartphones awaiting assignment or prior to transfer for barcoding.
- 1.3 Evaluate existing or new software capabilities for managing asset tracking numbers to ensure consistent classifications and account for all assigned asset numbers.
- 1.4 Require asset barcoding for smartphones.
- 1.5 For all mobile computing devices, strengthen documentation requirements to track the transfer of asset custody, disposition status and method. Asset records should provide management with reliable information on the status and location of all tracked assets.
- 1.6 Provide detailed transfer records to Warehouse staff that allows them to verify devices transferred for surplus auction, such as model and serial numbers. Where feasible, also provide device condition information to support the Warehouse's auction process.
- 1.7 Establish and document disposition procedures for mobile phones. Procedures should address secure storage of the devices and require documentation of disposition methods.
- 1.8 Adopt a formal replacement policy for smartphones and tablets that consider operating system and security support limits. Review the existing inventory and identify devices outside of those requirements that are due for replacement.

2. Mobile devices are managed across multiple systems, creating inefficiencies and inconsistent processes.

City processes for approving, issuing, and tracking mobile devices rely on a mix of systems as illustrated by Figure 4 on page 9. Device-related records were maintained in multiple systems and some changes relied on email, leading to inefficiencies and inconsistencies in the data between systems. At the time of this audit, the IT department was in the process of implementing a new IT service management system to replace the current system, Cherwell. However, the initial implementation would not include mobile phone assets. Additionally, mobile phone records are split and maintained separately based on the carrier. Centralizing mobile phone assets in the primary asset management system could help streamline processes and improve data accuracy and reliability.

A. Mobile phone inventory records are maintained in multiple systems separate from the central IT asset management system and procedures may vary.

The City uses two service carriers for voice and data services: Verizon and AT&T. Verizon device records are maintained in WTS while AT&T devices are not. The AT&T inventory

listing, comprised of devices used by the Police Department, is only maintained on the provider's web portal. Established policies refer to WTS as the centralized mobile phone inventory and procedures do not reflect differences for AT&T devices.

Specifically, roles and responsibilities for managing AT&T inventory records have not been clarified, and procedural steps have not been documented. Initial audit interviews with the Wireless Administrator indicated that the Police Department was able to access the AT&T records and review active phones and user assignment; however, according to Police Department staff they did not have access to the records. Further, as noted in Finding 1, it is unclear how retired devices are recorded in AT&T. The inventory data we received showed only active lines and assigned users, but no details about device serial numbers, date of issuance, and prior user

assignments. These limitations are likely because the AT&T web portal is not intended to function as an asset management tool.

Systems Containing Mobile Phone Records

- **Wireless Tracking System (WTS):** A city-developed system used to track all mobile phone usage authorizations, and Verizon phone inventory records, monthly charges, and call history.
- **Verizon web portal:** Service carrier website for managing service lines and viewing monthly charges.
- **AT&T web portal:** Service carrier website for managing service lines and monthly charges. Contains some asset information, such as assigned user and device model.
- **Intune:** Used as the mobile device management system (MDM) to manage security configurations and remote wipe devices as needed. Only Apple phones and tablets are currently managed through Intune.

Figure 4. Mobile device processes are managed across multiple systems.

Description	Smartphones	Tablets	Laptops
Request for device issuance	WTS	Cherwell	Cherwell
Approval of initial request	WTS	Email	Email
Request for changes (i.e., replacement devices, reassignments, cancellations)	Email	Email	Cherwell
Approval of changes	Email	Email	Email
Service tickets for provisioning and other changes	Cherwell	Cherwell	Cherwell
Configuration management	Intune	Intune	Cherwell and various
Asset Inventory	WTS AT&T portal	Cherwell	Cherwell

SOURCE: Auditor analysis based on staff interviews, process walk-throughs, and documentation review.

B. Decentralized asset records make managing service requests difficult, contribute to data discrepancies, and hinder effective monitoring of compliance with security standards.

Technology service requests are managed through Cherwell to route work to the responsible teams and track completion. As noted above, mobile phone asset records are not maintained in Cherwell, unlike laptops, tablets, and other technology assets. This creates inefficiencies and makes monitoring changes more challenging.

1. **Changes must be entered in multiple systems** – For new or changing mobile phone assignments, the Wireless Administrator must enter a Cherwell service request for IT Technicians to initiate device set-up and configuration in the mobile device management system (MDM), Intune, before a phone can be issued. The Wireless Administrator must also update WTS and the cellular service provider's web portal, resulting in duplicative data entry.
2. **Lack of audit trail for change requests** – Work order service history is not easily tracked for mobile phones because the asset records is not in Cherwell. Further, all other phone change requests, such as device upgrades, user assignments, replacement phones, and line suspensions, are typically initiated through email instead of a service request. The Wireless Administrator creates an IT service ticket on behalf of the client department. We were unable to verify whether this occurred consistently because the original requests are only stored in the Administrator's email, and the employee was out on leave during much of the audit.
3. **Ineffective monitoring of device compliance** – Our review of the MDM system data for managed devices showed significant differences from the WTS device data, indicating that service tickets were not consistently entered to notify IT Technicians of required changes. Outdated or inaccurate device information in the MDM prevents effective monitoring of security configuration compliance:
 - About 6% of the approximately 1,200 smartphones enrolled in the MDM appeared to be inactive because there were no associated cellular service charges for the phone line. Additionally, about 170 phone lines had multiple devices registered because previously retired devices had not been unenrolled.
 - The assigned primary user in the MDM did not always match the assigned user in WTS.
 - Device non-compliance with established security configurations initially appeared high, at 26%; however, when removing potentially outdated records, we estimated non-compliance was about 11%.

C. Compliance with required Wireless Service Use Agreements is difficult to verify, and more frequent acknowledgement of use policies would ensure employees are aware of changes to expectations.

To be issued a City mobile phone, employees must sign a use agreement that outlines acceptable uses, employee responsibilities, and affirms compliance with City technology policies. The use agreements and supervisory approvals are managed in WTS through an approval workflow that routes authorization to the employee's identified

managers. However, a process has not been established to verify that all active users have a signed and approved agreement.

- WTS data does not link the user agreement approval information to device user data.
- Further, AT&T devices and assigned users are not entered into WTS.

Existing policies only require a signed Agreement when the employee is initially authorized for a phone. For employees who have had city-issued phones for many years, this means newer or updated policies may not have been acknowledged, and the original agreement may not be retained in WTS. Although recurring supervisory approval may not be necessary, a more frequent interval for review and acknowledgement of user agreements would ensure employees are aware of the most current acceptable use policies.

D. Minor exceptions were noted relating to missing documentation and lack of supervisory approvals for smartphone issuance.

City policy requires that all city-owned mobile phones be requested through a WTS Request Form, including a documented business justification, receive level-one (director) approval and include a user-signed Wireless Service Use Agreement prior to device issuance. A review of about 250 WTS service requests created in FY 2025/26 found that while most requests complied with City policies, 8 requests had the following exceptions:

- Six users approved their own mobile phone authorization (no manager approval).
- One user was approved without a signed use agreement.
- One use agreement was signed by the department coordinator rather than the assigned user.

Recommendations

The IT department should:

- 2.1 Explore options for consolidating mobile device records into a single platform to streamline procedures and reduce data errors and inconsistencies. As the department implements the new IT asset and service management system, consider including smartphones in that implementation to centralize asset records and improve tracking of service requests.
- 2.2 Review devices enrolled in the MDM system to ensure inactive devices are removed and other information is up to date.
- 2.3 Establish a procedure to verify that all active mobile phone users have signed Use Agreements. Require authorized employees acknowledge mobile phone use policies on an annual or other regular interval.
- 2.4 Review and update policies and workflow rules to ensure that mobile phone requests are appropriately authorized.

3. About 4% of mobile phone service lines were associated with terminated employees, and information for review of other device charges is insufficient.

The City spends approximately \$1.4 million annually on cellular voice and data services for mobile computing devices. Our review found that processes for communicating changes to employee status or device assignment and reviewing monthly charges could be improved to minimize potential overpayment of unnecessary services. Additionally, services purchased through cooperative agreements need to be approved by the Purchasing department.

A. About 4% of mobile phone lines were associated with terminated employees; improving employee transfer and off-boarding procedures could help ensure timely suspension of services and accuracy of custody records.

Some missed mobile phone changes to device assignment or status are caught during an annual review, when the IT Wireless Coordinator sends each department coordinator a listing of their mobile phones and users for verification. However, some changes are still not identified, and delays in line suspensions can result in unnecessary charges.

We reviewed one recent month of service charges and found that about 4% of mobile phone lines for the approximately 1,200 phone lines were associated with terminated employees (an estimated cost of \$2,000 per month). For 26 of these, auditors followed up with department coordinators and found the following procedural gaps:

1. **Untimely or missing notifications to IT** – In 12 instances, there was no indication that the coordinators notified IT of the employee separation or request suspension or termination of the phone line. Three notifications were submitted significantly late, ranging from 55 to 237 days after the employee's departure or transfer. In one instance, an employee transferred to another department but the phone line remained active and the first department continued to be charged for monthly services.
2. **Untimely or incomplete suspension of line by IT** – In 7 instances, the Wireless Administrator received notification and changed the device status in WTS but did not suspend the service. In another 7 instances, the service was not suspended promptly (auditors applied 2 weeks of notice).
3. **IT was not notified of user assignment changes** – In 3 instances, the devices are associated with terminated employees. Auditors found that the assigned user had changed, but the department coordinator had not notified the Wireless Administrator of the user change.

Updating the off-boarding checklist and centralizing device assignment information would improve the client department's ability to consistently notify IT of device changes. Although the City's Employee Exit and Transfer checklist instructs supervisors to collect city-issued devices, the following gaps remain:

- Supervisors may not have information on all devices assigned to an employee or in their possession due to the lack of centralized asset inventory. Mobile phones inventories are maintained separately in two systems from other technology assets with inconsistent updates to assigned user data.

- The checklist does not address notification to IT of changes in user assignment or physical custody of devices to ensure accountability for the asset, and temporary suspension of cellular service as needed when the assigned user terminates or transfers.

In addition to providing a centralized inventory of technology assets, tracking mobile phone devices and service requests through the service management system (as recommended in Finding 2) would improve oversight of off-boarding actions and allow monitoring of timely completion. As well, department coordinators could submit their own service tickets for device changes, reducing duplication of effort.

B. Most monthly service charges were only reviewed for reasonableness.

The City spends approximately \$1.4 million each year on cellular voice and data service. For phone lines managed in WTS (about 600 Verizon voice and data lines), the Wireless Administrator performs a comparison of the active lines billed to ensure they are also active in WTS. However, about 600 AT&T voice and data lines and another 1,800 data-only lines for tablets, laptops, and other devices were not regularly validated against supporting information when approving monthly invoices for payment. Instead, monthly invoices are approved if the total amount is reasonable compared to prior billed amounts.

1. **Responsibility for review of AT&T charges need to be clarified** – According to initial audit interviews, the IT Wireless Administrator believed the Police Department coordinator had access to the AT&T web portal to review the active accounts and charges. However, according to the Police Department, they did not have access to the web portal. When asked to review 19 no-usage accounts this past July, the coordinator identified lines associated with broken devices, terminated staff, and users with multiple lines.
2. **Vague or incomplete device descriptions made validation of cellular data charges difficult without a tracking method** – The IT department did not have a process for reconciling the service charges to devices approved for cellular data service. Although asset barcodes are now entered in the line description, staff noted this was not done consistently in prior years. Auditor review of the April 2026 bill totaling about \$69,000 showed that 43% of the nearly 1,800 accounts (or about 780) did not contain identifying device barcodes.

Using other asset data to validate some of the missing device information, auditors were able to identify 71% of the billed service lines. However:

- About 60 of these lines were associated with devices that had not communicated with the Mobile Device Management system in over 6 months or had a disposition/surplus status. We were able to confirm that 27 of these devices are still deployed but have not been recently used.
- Three others had incorrect barcodes assigned to desktop computers rather than laptops.

Of the remaining approximately 520 lines with insufficient information to identify the device to asset records, 132 did not have any reported data usage in the month reviewed.

3. **Data charges for laptops and tablets varied, and information regarding plan selections was not documented** – While the voice and data provider contract has a long list of plan options, about 40% of the approximately 1,800 service lines were billed at \$20 per month, and 55% were at \$39.99 per month. The remainder had other rates that appeared to be partial-month charges or mobile hot spot devices. According to the department, the cost difference was based on the device model or capabilities, with newer 5G devices qualifying for the \$20 plan. However, the selected plan for each device was not documented.

As illustrated by Figure 5, our review of the charges with device information found multiple instances where the same model device had different monthly costs. According to IT staff, except for Panasonic FZ55-2, all laptops listed in the figure should be in a \$20 plan. It was further noted that the two different plans (\$20 and \$39.99) were introduced around the same time, and there may have been some confusion about which one to choose. Identifying the city-approved plan options and documenting the specific plan selected for each device would allow staff to more accurately validate monthly service charges.

Figure 5. Examples of same-model devices with different data plan costs.

Description	\$20 Monthly Plan	\$39.99 Monthly Plan
Laptops		
Panasonic FZ55-2	1	153
HP Elite X360 G10 2-IN-1 Notebook	30	29
HP Elitebook G10 Notebook	1	43
HP Elitebook 650 G9 Notebook	83	40
Tablets		
iPad - 10 th Generation	162	89
iPad - A16	2	1

SOURCE: Auditor analysis of Verizon data bill for the month ending April 16, 2026, and device information from the asset management system and the mobile device management system.

C. Cooperative purchasing contracts for voice and data services lacked required Purchasing review to ensure that the procurement process and contract terms met City policy.

The IT department uses two contracts procured by a cooperative purchasing organization to obtain voice and data services, as well as phones, tablets, and other related equipment. The City's Procurement Code allows this type of purchase with review and approval from the Purchasing Director. However, the only approval on record was for the Police Department's use of the AT&T contract for emergency mobile hot spots.

The Purchasing department's review and approval helps ensure that the cooperative contract is advantageous for the City, and that the procurement meets the purpose and spirit of the City's Code. Additionally, Purchasing may require the vendor to sign a city services contract to accept standard city terms.

Cooperative purchasing contracts are issued for use by other government entities and are procured by a cooperative purchasing organization or consortium, or another government entity, such as the State of Arizona.

SOURCE: Auditor summary of Procurement Code, section R2-191.1

Recommendations:

The IT department should:

- 3.1 Work with Human Resources to update the Employee Exit and Transfer Checklist to address procedures related to mobile devices, such as verifying all assigned devices have been returned, notifying the appropriate contact regarding transfer or reassignment of the devices and suspension of service. Require the related service requests to be submitted in the IT service management system to allow for tracking of service completion.
- 3.2 Establish an escalation policy to address noncompliance with mobile device policies.
- 3.3 If consolidation of mobile device records is not feasible, update policies and procedures to address AT&T mobile phone records that are not maintained in WTS.
- 3.4 Establish procedures for verifying accuracy of monthly service charges, such as developing a tracking tool with the active device numbers, authorized users, and monthly plan costs for comparison against monthly invoices. To facilitate process automation, the department should update information in the cellular provider's system to ensure descriptions have device barcodes and usernames. Additionally, review assigned data plans and update plans as needed.
- 3.5 Obtain Purchasing department's review and approval for all cooperative contracts.

4. Review of technical and security controls identified several high or critical priority areas.

Protiviti conducted a review of technical and security controls governing the City's managed mobile computers and devices. The audit team's findings and observations were provided to the IT department for remediation but are not detailed here due to the potentially sensitive nature of security-related findings. Several areas identified as high or critical priorities for remediation are summarized below:

- Conditional Access policies need to be reviewed and updated to address several identified configuration gaps.
- A comprehensive review of configuration settings in the Mobile Device Management system is needed to address identified gaps in alignment with recommended technical security standards.
- Security configuration benchmark exceptions for managed laptops need to be addressed.

- For managed mobile devices, security configuration profiles should be re-built to align with a recognized industry benchmark, such as CIS Benchmark for iOS and iPadOS.
- Controls are needed to ensure that vulnerability remediation activities follow the timeframes defined in the Vulnerability Management Policy.

Recommendation:

The IT department should implement the recommendations identified in the detailed Protiviti report.

METHODOLOGY

To achieve the audit objectives, the following procedures were performed:

- Reviewed applicable governance and policy including city administrative rules, IT adopted policies and mobile device guidance. Among others, key Administrative Regulations and IT policies included:
 - AR 106 City-owned Cellphone, Smart Device Issuance & Usage
 - AR 136 Network and Computer Security
 - AR 128 Personal Electronic Communication Device Usage
 - New Equipment Inventory Policy
 - Criteria for Barcoding IT Equipment Policy
 - Smartphone Replacement Policy
- Performed walkthroughs and interviews with key IT staff involved in all phases of the asset management lifecycle.
- Reviewed workflow documentation, user guides, and systems of record supporting the city's mobile-device processes across multiple systems.
- Obtained and analyzed asset data from the following sources:
 - Wireless Tracking System, an internal application developed to track city mobile phones. Data reviewed included user authorization requests and asset inventory records.
 - Reports from the AT&T web portal on active users and devices.
 - Cherwell (the asset management and IT service management system) asset records for mobile devices, which included laptops and tablets, as well as service records and asset status changes for these devices.
 - Microsoft Intune, the mobile device configuration management system.
- Reviewed voice and data service invoices for mobile computing devices, including mobile phone service and data plan costs for laptops and tablets. We evaluated management control over the review and payment of these invoices and compared the billed charges to city records on active devices and user assignments.

To evaluate technical and security controls, the Protiviti team applied the following industry frameworks in their risk assessment:

- Center for Internet Security (CIS) Controls v8.1
- National Institute of Standards and Technology (NIST) publications SP 800-124 Rev. 2 and SP 800-53 Rev. 5

Their review covered the following nine control domains:

- Governance and policy
- Asset inventory and visibility
- Device configuration and hardening
- Identity and access management
- Data protection
- Application security
- Network security
- Monitoring, logging and device detection
- Incident response

Audit Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 work took place from May to September 2026.

MANAGEMENT ACTION PLAN

1. Stronger receiving and disposition controls are needed to ensure accountability and safeguard mobile computing assets.

Recommendations

The IT department should:

- 1.1 Assess and update internal procedures to ensure adequate separation of duties for the ordering, receiving, and recording of mobile phones and tablets. Procedures should also ensure that purchases of equipment have approved requisitions and receiving documentation prior to invoice payment.
- 1.2 Require secure storage for tablets and smartphones awaiting assignment or prior to transfer for barcoding.
- 1.3 Evaluate existing or new software capabilities for managing asset tracking numbers to ensure consistent classifications and account for all assigned asset numbers.
- 1.4 Require asset barcoding for smartphones.
- 1.5 For all mobile computing devices, strengthen documentation requirements to track the transfer of asset custody, disposition status, and method. Asset records should provide Management with reliable information on the status and location of all tracked devices.
- 1.6 Provide detailed transfer records, such as model and serial numbers, to Warehouse staff that allows them to verify devices transferred for surplus auction. Where feasible, also provide device condition information to support the Warehouse’s auction process.
- 1.7 Establish and document disposition procedures for mobile phones. Procedures should address secure storage of the devices and require documentation of disposition methods.
- 1.8 Adopt a formal replacement policy for smartphones and tablets that consider operating system and security support limits. Review the existing inventory and identify devices outside of those requirements that are due for replacement.

Management Response:	Management acknowledges and agrees with the recommendations outlined in the audit report. Recognizing the importance of effective asset lifecycle management, we are committed to strengthening internal controls, improving inventory accuracy and accountability, and establishing consistent procedures to ensure the city appropriately manages, safeguards, and disposes of its mobile computing devices.
Proposed Action:	The Information Technology Department will implement a phased approach to strengthen asset receiving, inventory tracking, custody, and disposition practices. This effort will include establishing standardized asset identification and documentation requirements, strengthening segregation of duties and physical security controls, improving the tracking and verification of asset transfers and disposals, and reviewing device replacement practices to ensure continued operational and security compliance. These

	improvements will enhance accountability, reduce the risk of asset loss, and establish a more consistent, transparent approach to managing mobile computing devices throughout their lifecycle.
Est. Completion Timeframe:	May 2027
Responsible Party:	Information Technology Department, in coordination with the Purchasing and impacted departments.

2. Mobile devices are managed across multiple systems and platforms, creating inefficiencies and inconsistent processes.

Recommendations

The IT department should:

- 2.1 Explore options for consolidating mobile device records into a single platform to streamline procedures and reduce data errors and inconsistencies. As the department implements the new IT asset and service management system, consider including smartphones in that implementation to centralize asset records and improve tracking of service requests.
- 2.2 Review devices enrolled in the MDM system to ensure inactive devices are removed and other information is up to date.
- 2.3 Establish a procedure to verify that all active mobile phone users have signed Use Agreements. Require authorized employees acknowledge mobile phone use policies on an annual or other regular interval.
- 2.4 Review and update policies and workflow rules to ensure that mobile phone requests are appropriately authorized.

Management Response:	Management acknowledges and agrees with the recommendations outlined in the audit report. We recognize the importance of maintaining accurate, consistent, and accessible asset information across the organization and are committed to improving the integration of technology management systems, standardizing operational processes, and strengthening governance over mobile computing devices.
Proposed Action:	The Information Technology Department will evaluate opportunities to consolidate and streamline mobile device asset management through existing enterprise platforms and improved system integration. This effort will focus on establishing a more centralized, reliable inventory; standardizing device provisioning and assignment workflows; improving visibility into device ownership and compliance; and strengthening the administration and acknowledgment of mobile device use agreements. Where appropriate, the

	department will leverage workflow automation and enhanced reporting capabilities to reduce manual processes, improve data accuracy, and establish consistent accountability across departments.
Est. Completion Timeframe:	October 2027
Responsible Party:	Information Technology Department, in coordination with impacted departments.

3. About 4% of mobile phone service lines were associated with terminated employees and review of other data charges is insufficient.

Recommendations

The IT department should:

- 3.1 Work with Human Resources to update the Employee Exit and Transfer Checklist to address procedures related to mobile devices, such as verifying all assigned devices have been returned, and notifying the appropriate contact regarding transfer or reassignment of the devices and suspension of service. Require the related service requests to be submitted in the IT service management system to allow for tracking of service completion.
- 3.2 Establish an escalation policy to address noncompliance with mobile device policies.
- 3.3 If consolidation of mobile device records is not feasible, update policies and procedures to address AT&T mobile phone records that are not maintained in WTS.
- 3.4 Establish procedures for verifying accuracy of monthly service charges, such as developing a tracking tool with the active device numbers, authorized users, and monthly plan costs for comparison against monthly invoices. To facilitate process automation, the department should update information in the cellular provider's system to ensure descriptions have device barcodes and usernames. Additionally, review assigned data plans and update plans as needed.

Management Response:	Management acknowledges and agrees with the recommendations outlined in the audit report. Recognizing the importance of fiscal stewardship and effective oversight of mobile communications expenditures, we are committed to strengthening the processes governing cellular service assignments, employee separations, billing reconciliation, and ongoing service utilization to ensure appropriate accountability and cost management.
Proposed Action:	The Information Technology Department will collaborate with Human Resources, Purchasing, and impacted departments to strengthen controls governing cellular services and associated expenditures. Improvements will include enhancing employee separation and transfer procedures to ensure

	timely notification and disposition of assigned devices and services, establishing recurring reconciliation and validation of cellular service records and billing, and implementing appropriate exception management and escalation procedures. The department will also review cellular service utilization, plan assignments, and procurement practices to identify cost-optimization opportunities, eliminate unnecessary expenditures, and improve the accuracy and transparency of mobile communications costs.
Est. Completion Timeframe:	October 2027
Responsible Party:	Information Technology Department, in coordination with Human Resources, Purchasing, and impacted departments.

4. Review of technical and security controls identified several high or critical priority areas.

Recommendations

The IT department should implement the recommendations identified in the detailed Protiviti report.

Management Response:	Management acknowledges and agrees with the recommendations identified in Protiviti's detailed technical security assessment. Recognizing the importance of maintaining a resilient and secure technology environment, we are committed to addressing identified security gaps, strengthening mobile device management controls, and continuously improving the city's cybersecurity posture in alignment with established security policies, standards, and risk management practices.
Proposed Action:	The Information Technology Department will adopt a coordinated, risk-based approach to implementing the recommendations identified in the report. The department will prioritize remediation activities based on severity, potential impact, and operational dependencies, with an emphasis on strengthening access controls, security configurations, device compliance, and vulnerability management practices. A structured remediation plan will establish ownership, implementation milestones, and validation procedures to ensure the city systematically addresses identified risks.
Est. Completion Timeframe:	October 2027
Responsible Party:	Information Technology Department in coordination with impacted departments.

City Auditor's Office

Lai Cluff, Acting City Auditor
Elizabeth Brandt, Senior Auditor
Allison McLeod, Senior Auditor
Wenhao Wang, Senior Auditor
Shelby Trimaloff, Exec Asst to City Auditor

Audit Committee

Councilman Barry Graham
Councilwoman Maryann McAllen, Chair
Councilwoman Solange Whitehead

Our Mission

*The City Auditor's Office conducts audits to promote operational efficiency,
effectiveness, accountability and integrity in City Operations.*

Scottsdale City Auditor

7447 E. Indian School Rd. | Suite 205 | Scottsdale, Arizona 85251
OFFICE (480) 312-7756 | INTEGRITY LINE (480) 312-8348
www.ScottsdaleAZ.gov/auditor

