**Office of the City Auditor
Kansas City, Missouri**

Highlights

Why We Did This Audit

Mobile devices may expose the city to new security risks, such as downloading malware to the city's devices and network or exposing confidential or personally identifiable information. Security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile devices, and mobile device operating systems are not updated as frequently as those on personal computers and laptops. Security threats to mobile devices also include loss or theft, unauthorized access to networks or data, and the ability to identify user location.

Our audit focused on reviewing security practices on smartphones and tablets used for city business.

Background

Mobile devices are portable computing devices that allow users to access data, email, the Internet, GPS navigation, and other applications remotely. The city owns over 750 smartphones and tablets used by employees for city business.

Employees who need a cellphone for city business and want to use it for personal use have two options; (1) use a city-owned cellphone and pay a portion of the usage cost or (2) use their personal cellphone and receive a stipend to defray the cost of using it for city business. There are about 230 personally owned cell phones used for city business.

For more information, contact the
City Auditor's Office at 816-513-3300 or
cityauditor@kcmo.org.

🐦 @KCMOCityAuditor

To view the complete report, go to
kcmo.gov/cityauditor
and click on Search Audit Reports.

PERFORMANCE AUDIT
Mobile Device Security Risks

What We Found

Mobile devices are subject to numerous security threats. Although the city has some mobile device security policies, it lacks some critical policy requirements to mitigate mobile device security vulnerabilities, such as requiring operating system updates, disabling location services when not in use, immediately reporting lost devices to IT, establishing safeguards for syncing and backing up mobile devices used for city business, and requiring encryption on data stored on Surface tablets.

Although city policies require some key security features to be implemented on users' mobile devices, not all users of city smartphones and tablets are following them. Not all mobile devices used for city business require a passcode to access; users are not disabling Bluetooth functionality when the function is not in use; and city policy is not clear on what types of app stores users should avoid. City employees do not receive much mobile device security training to ensure the mobile device users understand the importance of mobile device security requirements and how to follow the requirements.

The city does not have a mobile device management software as recommended to enforce key mobile data security features. Any mobile device with unimplemented security safeguards leaves a hole in the city's defense against unauthorized access to city data or can lead to harm to the city's information systems.

What We Recommend

We make recommendations to ensure city data accessed by, and stored on mobile devices is more protected by:

- Updating city policies to include key mobile device security requirements,

- Training employees to set security features on their mobile devices and understand why the security features are important, and

- Implementing MDM software to protect city data and enforce security requirements.

Management agreed with all the recommendations.