Office of the City Auditor
Kansas City, Missouri

Highlights

Why We Did This Audit

The city's identity and access management affect the security of all network users, devices, and applications. It should provide reasonable assurance that users have the appropriate authentication and authorization.

Access by unauthorized users could result in loss of data, disruption of city business, and disclosure of sensitive information. The city may incur loss of and damage to reputation, public trust, regulatory compliance, business continuity, and money.

Objective

This audit focuses on whether computer network accounts to the city's information technology network are current.

Background

The Information Technology Division is responsible for the security of most of the city's network of computers and peripheral devices. The division is responsible for providing authorized users with secure IT services and granting appropriate access to the network.

Identity and access management of the city's computer network is used to ensure only authorized users have appropriate access to the computer networks, applications, processes, and data. This protects against unauthorized modification, loss, and disclosure of data; limits access to very sensitive resources, such as operating systems and security software programs; and restricts users from performing incompatible duties or duties beyond their responsibilities or authorizations.

To view other audit reports, please visit our website http://kcmo.gov/cityauditor and click on Search Our Work.

PERFORMANCE AUDIT

Network Accounts Not Current, Updating and Monitoring Needed

What We Found

Network accounts for some terminated employees have not been disabled. Information Technology Division (ITD) management said these accounts were still enabled because they had not been notified by these employees' departments.

Administrative Regulation (AR) 1-16, states "all additions/changes/removals of access to technology assets must be submitted in a timely manner to the Customer Service Center." The AR does not state what management considers to be "timely" and does not state how departments should notify ITD.

Disabling employee network accounts immediately after an employee leaves the city is important because hackers or disgruntled former employees could use these accounts to steal, destroy, or ransom sensitive data.

What We Recommend

To reduce the risk of terminated employee accounts being exploited for malicious purposes, we recommended:

- disabling accounts of all terminated employees.
- establishing written procedures to monitor network accounts.
- revising AR 1-16 to include the number of days after employee termination for departments to submit ITD's termination of computer account forms to the division.

Management agreed with the recommendations.

Closed Record

Our audit identified additional areas for improvement and management agreed or partially agreed with the recommendations. We are not publicly disclosing these details because of the sensitivity of this information and security concerns. The full audit report is a closed record under RSMo §610.021(21).