Highlights

Why We Did This Audit

The city collects and maintains personally identifiable information in both electronic and paper formats. Protecting this information concerns both individuals and the city. Loss, misuse, or unauthorized disclosure of personally identifiable information could cause serious harm to employees, residents, and the city. Individuals could suffer embarrassment, inconvenience, and fraud. The city could lose the public's trust and confidence, face legal liabilities, and pay to remediate problems.

Background

Personally identifiable information is any information that can be used to identify an individual or can be linked to an individual. Examples of personally identifiable information include names, addresses, social security numbers, date and place of birth, photos, financial account numbers, medical information, and employment information.

Audit Methodology

As part of our audit, we reviewed practices recommended by National Institute of Standards and Technology and other organizations. We also conducted an on-line survey about the city's practices in protecting personally identifiable information from loss, misuse, or unauthorized disclosure.

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

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

PERFORMANCE AUDIT
The City Should Follow Recommended Practices to Protect Personally Identifiable Information

What We Found

All city departments that responded to our survey collect and store at least two types of personally identifiable information we asked about and many store and collect four or more.

Selected Types of Personally Identifiable Information Collected and Stored by Departments

Type of Information	Number of Departments
Date of Birth	19
Social Security Number	18
Medical Information	16
Bank Account Information	14
Credit Card Number	9

Although the city collects a variety of personally identifiable information, it has not identified all that it collects, uses, and stores. Managing personally identifiable information by regularly reviewing what the city collects to determine whether the information is still needed for city business purposes can limit exposure if a breach occurs.

The city does not have citywide policies and procedures for protecting personally identifiable information. Roles and responsibilities for protecting the information are not clear. Some departments reported following federal or state regulations related to the information they collect, use, and store. Currently, the city has some policies and procedures in place to cover some aspects of personally identifiable information, but they are not enough to cover every stage of protecting personally identifiable information, including collection, access, storage, and disposal.

The city's training effort for handling personally identifiable information is fragmented. The city uses some recommended methods to protect confidential information, such as restricting physical access, destroying hard drives of retired computers, and encrypting some laptops, but safeguards for protecting personally identifiable information need to be increased.

The city needs to implement an incident response plan to ensure it responds to breaches involving personally identifiable information quickly, consistently, and effectively.

What We Recommend

Our recommendations are directed towards improving how the city protects personally identifiable information by:

- Identifying what information the city collects.
- Periodically reviewing and eliminating unnecessary collection and retention.
- Developing citywide policies and procedures, including training staff and applying safeguards.
- Developing an incident response plan.

Management agreed with the recommendations.