PERSONALLY IDENTIFIABLE INFORMATION INTERNAL AUDIT

November 2017

RubinBrown LLP
Certified Public Accountants & Business Consultants

One North Brentwood
Saint Louis, MO 63105

T 314.290.3300
F 314.290.3400

W rubinbrown.com
E info@rubinbrown.com

September 12, 2018

Finance and Administration Committee
City of Springfield
840 Boonville Ave.
Springfield, Missouri 65802

Re: Personally Identifiable Information (PII) Internal Audit

Dear Committee Members:

In conjunction with our overall engagement to provide internal audit services to the City of Springfield ("City"), we have completed our internal audit on the processes to obtain, store and dispose of personally identifiable information and the associated internal controls. Our services were performed in accordance with the International Standards for the Professional Practice of Internal Auditing, as promulgated by the Institute of Internal Auditors (IIA).

The accompanying report includes an Executive Summary, our Observations and Recommendations and Process Improvement Opportunities. Because the procedures performed in conjunction with the review are more limited than would be necessary to provide an opinion on the system of internal accounting controls taken as a whole, such an opinion is not expressed. In addition, the engagement did not include a detailed audit of transactions that would be required to discover fraud, defalcations or other irregularities.

This report is intended solely for the information and use of management and the City Council and is not intended to be, and should not be, used by anyone other than the specified parties. City of Springfield external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities. In addition, we understand that the City may be required to make our report, once finalized, available under sunshine laws.

We would like to express our gratitude to all employees involved with this project. Each person involved was accessible and responsive to our requests for information.

Sincerely,

RUBINBROWN LLP

Christina Solomon

Christina Solomon, CPA
Partner
Direct Dial Number: 314.290.3497
E-mail: christina.solomon@rubinbrown.com

Enclosures
cc: David Holtmann
Jody Vernon

CITY OF SPRINGFIELD
PERSONALLY IDENTIFIABLE INFORMATION INTERNAL AUDIT

Table of Contents

CITY OF SPRINGFIELD
Personally Identifiable Information Internal Audit
Executive Summary

Project Overview and Scope

We completed our audit of the processes to obtain, store, and dispose of personally identifiable information (PII) and the associated internal controls. The objectives of our audit were to:

- Ensure adequate internal controls exist over PII processes and are operating effectively.
- Evaluate PII processes for operating efficiencies and applicability of best practices.

Our scope was limited to determining if the following types of information are collected by the City:

Social Security Number	Credit Card Number
Date of Birth	Education Information
Bank Account Number	Medical Information

We did not review compliance with HIPAA laws and regulations as part of this audit.

Our audit included policies and procedures in place from July 1, 2016 through June 30, 2017. We completed the following procedures:

- Identified existing policies and practices in place for the processing and storage of PII.
- Performed in-person interviews with City personnel in the following departments: Police, Fire, Human Resources (HR), Municipal Courts, Information Systems, Health, Finance, Airport, Risk Management, Environmental Services, Art Museum, Parks, Planning and Development, Workforce Development, Legal, and Public Works. The objective of these interviews was to gain an understanding of the following:
  - Types of PII gathered by the City departments;
  - Inventory of PII stored and the process for destroying PII that is no longer relevant;
  - Incident response plan in place for PII incidents;
  - Protection and restriction of PII at various levels – databases, networks, system platforms, applications, and business processes/functional levels;
  - Disclosure of PII to third parties.
- Testing of transactions was not performed as part of this audit.

Background

The City's departments collect PII from both employees and citizens. Each department collects different types of information based on the services they provide. Information

can be collected by mail, in person, and electronically. Preferred methods of collection and strategies for PII protection vary by department.

Certain departments have PII policies or procedures that are applicable City-wide. For example, the Information Systems (IS) team manages the network and email for the City. IS has an incident response plan in place should any electronic PII be compromised through a data breach. The Finance department has a Financial Controls procedure in place for processing financial data. Also, City departments must adhere to the records management policy for records storage and destruction processes.

Best Practices

Based on our review, the City has adequate internal controls for PII, except as provided in our observations below. The following are some examples of the City's best practice internal controls:

- Human Resources department and Finance departments recently implemented physical access restrictions to the departments by using electronic badges.
- Most departments use a third party shredding company.
- Some departments have strong redaction procedures. For instance, the Parks department has a redaction marker, which completely obscures sensitive information.

Observations and Recommendations

We noted the following observations during our review:

- The City does not currently have a comprehensive policy to provide guidance on the collection, storage, and disposal of PII.
- The IS department has a plan for data breaches, however, the City does not have a written guide or policy for how to respond, in general, to a loss of PII.
- City departments are not required to use a third-party shredding company to dispose of sensitive information such as PII.
- A periodic review of the necessity of information collected from clients and employees is not performed by City departments.
- The Art Museum stores personnel files, which contain PII, onsite at the museum.

Additionally, we provided four process improvement opportunities below. All observations, recommendations, and process improvement opportunities were discussed with management. Details are noted in the tables attached immediately hereafter.

	Process/Procedure	Observation and Risk	Recommendation	Management Response
1	Various City departments have policies and procedures in place to provide guidelines on the collection, storage, and disposal of PII. For example, the Police, Fire, and Information Systems departments address different aspects of the PII lifecycle through individual department policies.	**Observation:** The City does not have a comprehensive PII policy that provides guidance on the collection, storage, and disposal of PII. **Risk:** Inconsistent treatment of PII, which could lead to violation of state law 407.1500, which requires notification of breaches.	Publish a comprehensive PII policy that addresses the collection, storage and disposal of PII. Department policies should be maintained, but revised if they conflict with the City-wide policy.	The City agrees with the recommendation. We will draft and publish a comprehensive PII policy addressing the collection, storage and disposal of PII. Employees will be required to undergo training on the policy every two to three years. Our target date to complete the policy is August 31, 2018.
2	The Information Systems department has an incident response plan that provides guidance on breaches of the City's network. Part of the plan requires documentation of PII lost as part of the breach.	**Observation:** A City-wide formalized incident response plan for responding to the loss of customer or employee PII does not exist. **Risk:** Response to loss of PII that does not comply with state law.	Create a detailed incident response plan for lost PII. This plan should provide step-by-step instructions for any City employee that discovers a data breach. The plan can be included as part of the City's comprehensive PII policy, or can be a separate document.	The City agrees with the recommendation. We will include a detailed incident response plan for lost PII and data breaches in our comprehensive PII policy. Our target date to complete the policy is August 31, 2018.

	Process/Procedure	Observation and Risk	Recommendation	Management Response
3	The City uses a third-party contractor, Shred-It, to collect sensitive documents for destruction. Most departments use the contracted document destruction services. However, the Art Museum, Planning & Development, and Public Works departments do not use the shredding service.	**Observation:** City departments are not required to use a professional shredding company to dispose of sensitive information. Therefore, we could not determine if sensitive documents were disposed of in an appropriate manner for the departments that do not use the third-party contractor. **Risk:** Loss of PII.	As part of the City's policy on disposal of PII, require that departments use the contractor for shredding services. If departments do not take part in the contract, require that sensitive information is destroyed using a micro-cut shredder prior to disposal.	The City agrees that all departments must have a secure method for disposing of sensitive documents. We will require all departments to use one of the City's contractors for shredding services or a micro-cut shredder as part of the comprehensive PII policy. Our target date to complete the policy is August 31, 2018. The Art Museum, Planning & Development, and Public Works will begin using one of the shredding services contracted by the City or a mircro-cut shredder. Our target date to complete this action is June 30, 2018.

	Process/Procedure	Observation and Risk	Recommendation	Management Response
4	Multiple departments within the scope of our review collect PII from clients: • Ten departments collect social security numbers, • Ten collect birthdates, • Nine collect banking information; and • Eight collect credit card numbers.	**Observation:** Currently, departments do not periodically assess the necessity of information they collect from clients or employees. **Risk:** Collection of PII that is not necessary and could subsequently be lost.	City departments should periodically (every two to three years) assess the information collected from clients and employees to determine if it is still necessary for operations.	The City agrees with the recommendation. The comprehensive PII policy drafted will charge departments with assessing the information collected from clients and employees every two years to determine if it is still necessary for operations. Our target date to complete the policy is August 31, 2018.
5	Human Resources serves as the central storage point for personnel information for the City. The employee's "permanent" file, which includes PII, is kept within the secure environment of Human Resources.	**Observation:** Currently some departments, such as the Art Museum, retain copies of employee personnel files on site. In all cases, the files are kept in locked cabinets. **Risk:** Loss of PII.	Store employee files in HR. Include as part of the comprehensive PII policy guidelines that sensitive employee information should not be stored at the individual department level.	The City agrees with the recommendation. The comprehensive PII policy will include guidelines that sensitive employee information should not be stored at the individual department level. Departments currently keeping copies of sensitive information contained in the employee HR files will securely shred that information. Our target date to complete the policy is August 31, 2018.

We noted the following process improvements during our review. These observations are not considered internal control weaknesses; however, we do recommend management consider each observation and take action where appropriate.

	Observation	Process Improvement	Management Response
1	Training for how to properly collect, retain, and dispose of PII is not required for City employees.	After implementing a comprehensive policy, periodically (every two to three years) train employees on the policy.	A mandatory training program will be established for employees as part of the comprehensive PII policy. Training will be required every two to three years.
2	File rooms and cabinets across the City are not always locked during business hours. Some of these cabinets are behind locked/secured doors, but some are not.	Each department should ensure that cabinets and file rooms that contain PII are kept locked except when they are in use.	The comprehensive PII policy will include a provision that departments ensure cabinets and file rooms containing PII are secured at all times.
3	Personally identifiable information collected by the Health department and Risk Management department may be disclosed to third parties as part of business operations.	Include a sentence on forms that indicates information collected could be released in the event of a health emergency (Health department) or insurance claim (Risk Management).	The Health Department will take the recommendation under advisement for the future. Risk Management will incorporate the recommended language on the claim form and the health authorization form immediately.
4	In some departments, such as the Municipal Court, clients are asked to orally provide their social security number.	Investigate the cost/benefit of implementing electronic key pads for clients to provide SSNs, or consider other ways to mitigate the risk of customers providing SSNs orally.	The Municipal Court will investigate the cost/benefit of implementing electronic key pads for clients to provide SSNs with consideration to the proprietary court software and hardware utilized.