FOLLOW-UP REPORT
Personally Identifiable Information in Salesforce
Technology Services
June 2019

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O’Brien, CPA
Denver Auditor
Audit Team
Brad Harwell, CIA, IT Audit Supervisor
Karin Doughty, CISA, Lead IT Auditor

Audit Management
Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, CMC, Deputy Auditor
Katja E. V. Freeman, MA, MELP, Audit Director

Audit Committee
Timothy M. O’Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ♦ Fax (720) 913-5253

Or download and view an electronic copy by visiting our website at: www.denverauditor.org.
AUDITOR’S LETTER

In keeping with generally accepted government auditing standards and Auditor’s Office policy, as authorized by city ordinance, the Audit Services Division has a responsibility to monitor and follow up on audit recommendations to ensure audit findings are addressed through appropriate corrective action and to aid us in planning future audits.

In our follow-up effort for the “Personally Identifiable Information in Salesforce” audit issued July 20, 2017, we determined the City’s Technology Services agency has adequately implemented five of the six recommendations made in the audit report. The remaining recommendation was partially implemented, in that Technology Services created a Salesforce user access report but did not distribute it to agencies for review. Despite Technology Services’ efforts, auditors determined the risks associated with the audit team’s initial finding have not been fully mitigated. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

The Highlights page in this report provides background and summary information about the original audit and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation.

I would like to express our sincere appreciation to the Technology Services personnel who assisted us throughout the audit and the follow-up process. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
Follow-Up Status
The City’s Technology Services agency (TS) has fully implemented five of the six recommendations made in the July 2017 audit report. One recommendation was partially implemented.

Objective
The objective of the audit was to assess the extent of unauthorized access to personally identifiable information (PII) in Salesforce, a customer relationship management (CRM) system.

Background
During continuous auditing work, Auditor’s Office personnel ran a query of Salesforce data to select a sample dataset for analysis. The access was mirrored to match that of a Denver 311 supervisor. Analysis of the sample file revealed that some description fields contained names, Social Security numbers, and birth dates. Although auditors sought a dataset limited to information obtained by Denver 311 operators, the query retrieved data entered into Salesforce by other agencies that also use it to manage customer interactions. Many of these entries were linked to the Department of Human Services (DHS) and the Payroll Division (Payroll).

REPORT HIGHLIGHTS

Highlights from Original Audit
We found assurance that TS assigned personnel with the appropriate experience to review Salesforce and its security capabilities when vetting possible choices to replace the City’s prior CRM tool. After performing a thorough evaluation, they determined that Salesforce could meet the City’s requirements for a vendor-hosted application.

We also confirmed that the third party that managed the Salesforce implementation process documented specific data security and privacy requirements for user data from both DHS and Payroll personnel who were explicit in requesting that their data, which includes PII, not be visible to other agencies. However, audit work revealed that sensitive information belonging to both DHS and Payroll was visible within Salesforce to a limited number of user profiles.

The Denver 311 supervisor profile, specifically, was configured with two settings that allowed the user of the profile to view all records in any City agency using Salesforce and to view all case data. Subsequently, two other user profiles were modeled after the Denver 311 supervisor profile and given view-all permissions to case data. The creation of profiles with such broad permissions was not in compliance with the security and privacy requirements for Salesforce submitted by DHS or the Payroll Division.

TS addressed the issue of unauthorized access prior to our completion of the audit. Although the Auditor’s Office did not participate in user acceptance testing, we did rerun the same Salesforce query seeking records containing PII. The resulting dataset contained significantly fewer records. After analyzing the data, we concluded that the few instances of PII that did show up were the result of citizens voluntarily giving their Social Security numbers during submissions of information to Denver 311 using the City’s pocketgov application.

Although TS addressed the immediate issue that led to the visible PII, we also noted areas where TS can strengthen its monitoring of the Salesforce contract to ensure continued adherence to required security practices. For example, TS is not reviewing attestation reports, which are required to be submitted by Salesforce annually. Reviewing this information would give TS assurance that Salesforce is continuing to adhere to its security policy and is positioned to identify and respond to security incidents, ultimately keeping the City’s data safe.

For a copy of this report, visit www.denverauditor.org or contact the Auditor’s Office at (720) 913-5000.
RECOMMENDATION — STATUS OF IMPLEMENTATION

FINDING – Technology Services Should Improve the Management and Administration of Salesforce

Recommendation

1.1 Salesforce Project Documentation – The Technology Services Project Management Office should ensure that Salesforce project documentation and artifacts are archived and readily available.

Status: Implemented (Original target date for completion: Agency response stated the agency had implemented this recommendation as of the issuance of the original audit report)

Agency Action

Technology Services originally identified SharePoint as the document repository for Salesforce projects, but the agency later selected another solution, Azure DevOps, after adopting what is called the “agile project management and software development methodology.” This method features shorter development cycles and frequent assessments of project deliverables, including regular meetings with the customer or stakeholder. This approach allows Technology Services to address agency concerns or enhancement requests on an ongoing basis. Azure DevOps documents the agency requirements including use cases (what the user can expect), the multiple iterations of the development process, and testing cycles. Although Azure DevOps tracks user acceptance testing results, the tool does not provide a module to record final stakeholder acceptance and approval.

Recommendation

1.2 Profile and Security Documentation – Technology Services should ensure that user profile security settings are documented and maintained for Salesforce administrators.

Status: Implemented (Original target date for completion: Agency response stated the agency had implemented this recommendation as of the issuance of the original audit report)

Agency Action

Technology Services deployed the Salesforce administration console, which provides access to user roles and sets of permissions. Salesforce administrators now have easy access to user security information.

In addition, Technology Services has migrated to a new Salesforce platform, called Lightning. Lightning has a restrictive access policy versus the traditional Salesforce platform, which has a permissive posture.
that grants permissions and does not expressly forbid access. Many of the existing applications were migrated to the Lightning platform, although a few still reside on the traditional platform.

Recommendation

1.3 Profile and Security Documentation – Technology Services should document information about Salesforce applications and specific security requirements for user agencies.

Status: Partially Implemented (Original target date for completion: March 31, 2018)

Agency Action

The Salesforce administration console allows a system administrator to create user reports, which include a user’s role and profile information for applicable Salesforce applications. Technology Services created a monthly active user report; however, the report has not been distributed to City agencies for their review, as stated in the management response from the original audit.

Reviewing active user reports informs agencies about the people who have access to their applications and the level of their access. This can be helpful in identifying employees who no longer need access because they transitioned to another role in the City. Technology Services relies on network access terminations to address the risk of unauthorized access by a terminated employee or a contingent worker. Salesforce was configured so when a terminated employee’s network access is removed, they can no longer access Salesforce. While this addresses the risk of unauthorized access for terminated employees, this does not mitigate the risk from employees who may have excessive access or employees who transfer to a new job in the City that no longer requires them to access Salesforce.

The overall risk was partially addressed because Technology Services has created two rules to help manage user access and licensing. The first rule will disable new user accounts not used within the first 48 hours of the account’s creation, and the allocated licenses will be returned to the pool of available licenses. The second rule disables accounts not used for 60 days and returns the allocated licenses to the pool of available licenses. According to the National Institute of Standards and Technology, the disabling of inactive accounts is a best practice and may ensure terminated or transferred employees’ user accounts cannot be used. However, this does not fully address the risk that a transferred employee may continue to have access to an application even if this is not required for their new position.

Recommendation

1.4 **Safeguard Citizen PII** – Technology Services should provide language on the Denver 311 webpage to inform citizens that sensitive personal data is not required and is discouraged when submitting an inquiry.

**Status: Implemented (Original target date for completion: March 31, 2018)**

**Agency Action**

Technology Services updated the City’s privacy and security policy to remind users of denvergov.org and its digital application that they should provide only the information required and requested and that they should avoid sharing unneeded personally identifiable information, such as Social Security numbers. Denvergov.org’s home page, the pocketgov website, and the Denver 311 webpage provide a link to the revised privacy and security policy. In addition, Technology Services added a message to the Denver 311 webpage that cautions users against providing unneeded personally identifiable information.

The City also established the Information Governance Committee to provide guidance to City agencies for how to handle protected data.

---

Recommendation

1.5 **Review Attestation Reports** – Technology Services should obtain and review Salesforce SOC 2 report, vulnerability scans, and penetration testing results on an annual basis to ensure that the vendor continues to provide secure services as required under the contract.

**Status: Implemented (Original target date for completion: March 31, 2018)**

**Agency Action**

Technology Services implemented a new module for vendor risk management in ServiceNow—the City’s system for entering, tracking, and updating information technology service requests. This module provides Technology Services personnel with the ability to track reviews of vendor Service Organization Controls reports and other security documentation. The module also provides them the ability to assign follow-up tasks to staff members and to track those tasks. Prior to using this module, Technology Services did not have a mechanism to track the reviews of Service Organization Controls reports; therefore, the 2019 review is the first documented review.

---

2 The Denver 311 Help Center receives inquiries, complaints, and requests about City services from Denver residents.

Technology Services told the audit team the next version of the module will allow the agency to create a task for reviewing Service Organization Controls reports on a recurring basis. Technology Services plans to expand the use of this module to track contract deliverables handled by the Salesforce contract application. This will allow the agency to centralize this functionality within one tool.

---

**Recommendation**

1.6 **Contract Tool or Process** – Technology Services should confirm that a process or tool for tracking deliverables and tasks related to contract management, including items such as insurance renewals and attestation reports received is implemented and working as intended.

**Status:** Implemented (Original target date for completion: March 31, 2018)

**Agency Action**

Technology Services developed a Salesforce application for contract management to assist the contract manager with key tasks, including monitoring expiration dates for both contract renewals and insurance certificates. The application provides automated notifications for renewals at multiple time intervals and allows the contract manager to upload related documents to the application.
CONCLUSION

While Technology Services has implemented five of the six recommendations made in the “Personally Identifiable Information in Salesforce” audit report, one recommendation has yet to be fully implemented. Despite the agency’s efforts, auditors determined the risks associated with the audit team’s initial findings have not been fully mitigated. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

On behalf of the citizens of the City and County of Denver, we thank staff and leadership from Technology Services for their cooperation during our follow-up effort and for their dedicated public service.
Office of the Auditor

The **Auditor** of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources. He also provides other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver’s government.

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City’s finances and operations, including the reliability of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000  ♦  Fax (720) 913-5253
www.denverauditor.org

**Our Mission**

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public’s investment in the City of Denver. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.