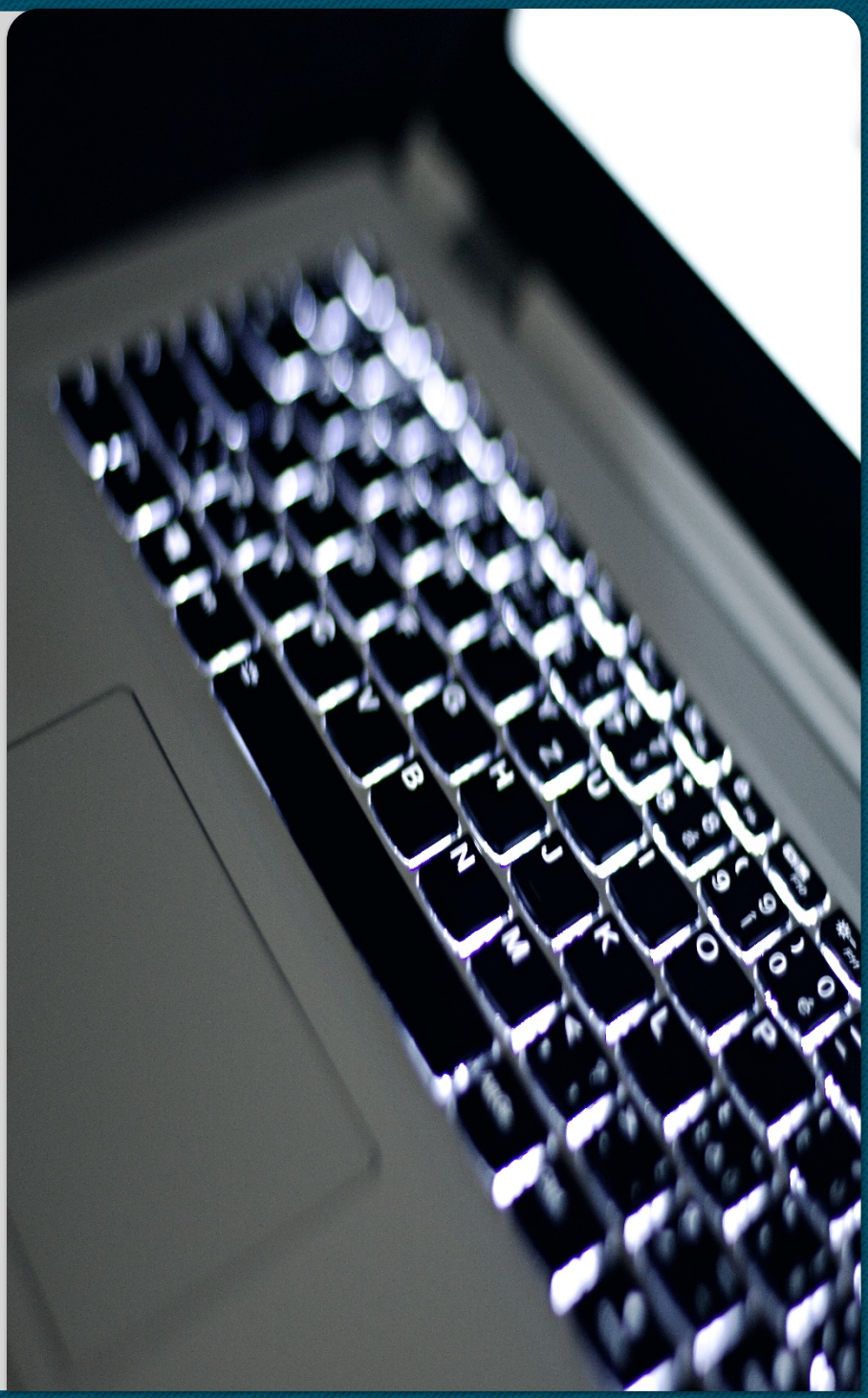
AUDIT REPORT
Technology Services – *Personally Identifiable Information in Salesforce*
July 2017



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

Timothy M. O'Brien, CPA
Denver 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 and providing 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.

Audit Committee

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

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Katja E. V. Freeman, MA, MELP, Audit Manager

Audit Staff

Shannon Kuhn, CISA, Audit Supervisor
Karin Doughty, CISA, Senior Auditor
Sam Gallaher, PhD, Data Analytics & Methodology Specialist

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) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
Report year: **2017**

Timothy M. O'Brien, CPA
Auditor

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202
720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

July 20, 2017

AUDITOR'S REPORT

We have completed an audit of Personally Identifiable Information (PII) in Salesforce. The objective of the audit was to assess whether PII stored in the Salesforce system was subject to unauthorized access. This audit was initiated by our office after discovering PII, to which we should not have had access, while performing audit work. Specifically, the data appeared in a report generated from data from the City's Salesforce system, which is a customer relationship management tool. Coming across sensitive personal information unexpectedly was greatly concerning to us, which is why we decided to perform a separate audit to uncover the root cause of the issue. We also notified the Mayor, the City's Technology Services department (TS), and other relevant parties immediately to prevent other users of Salesforce from unexpectedly stumbling upon this information, as we did. TS took quick action to secure this sensitive information.

We determined that the PII was accessible due to improper profile settings established in a limited number of Salesforce user profiles. We also determined that TS needs to improve the management and administration of Salesforce going forward. Through stronger administration of Salesforce security functions and increased emphasis on contract compliance, TS will be better positioned to safeguard PII stored in Salesforce. Our report lists several related recommendations.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, *General Powers and Duties of Auditor*, and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend appreciation to Technology Services and the personnel who assisted and cooperated with us during the audit.

Denver Auditor's Office

Timothy M. O'Brien, CPA

Auditor

PII in Salesforce
July 2017

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 the access that would be provided to a Denver 311 Supervisor. Through analysis of the sample file, we determined that some of the description fields contained names, social security numbers, and birth dates. Although the intent was to have a dataset limited to information obtained by Denver 311 operators, the query retrieved data entered into Salesforce by other agencies that also use this tool to manage their customer interactions. Many of these entries were linked to the Department of Human Services (DHS) and Payroll Division (Payroll). Subsequently, the discovery of this data was reported to the Mayor, Technology Services, DHS, and Payroll for further investigation and remediation.

REPORT HIGHLIGHTS

Highlights

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 within 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.denvergov.org/auditor or contact the Auditor's Office at 720.913.5000.

TABLE OF CONTENTS

BACKGROUND **1**

OBJECTIVE **4**

SCOPE **4**

METHODOLOGY **4**

FINDING **5**

Technology Services Should Improve the Management and Administration of Salesforce 5

AGENCY RESPONSE **12**

BACKGROUND

Salesforce is a cloud-based customer relationship management (CRM) tool that helps City and County of Denver (City) agencies to receive, manage, and store records of internal and external constituent inquiries, complaints, and requests. The Denver 311 Help Center (Denver 311) primarily receives these communications, both from citizens as well as City employees. The City selected Salesforce in 2014 to replace the City's prior CRM tool, which did not meet the City's requirements for enterprise reporting, was not very user friendly, and presented data security concerns. The purchase of Salesforce was funded by the City's Innovation Fund (iFund), which was established in 2012 to fund improvement projects that would measurably improve operations and service delivery within the City.

Salesforce is the City's customer relationship management (CRM) tool, which is used by the Denver 311 contact center to receive, manage, and store records of constituent inquiries.

Salesforce is intended to help the City increase the responsiveness of Denver 311 agents, improve the efficiency and performance of Denver 311's operations, and facilitate case intake and management. The system can accommodate a variety of communication vehicles, including telephone, email, web-based forms, live chat, and mobile-device applications. Depending on the type of support being provided by Denver 311 agents and other City agencies that use Salesforce to support constituents, the system can also interface with other tools, such as departmental work order systems and the City's geographic information system (GIS).

Other key benefits of Salesforce include enhanced reporting capability, data security improvements, and a user-friendly interface. The system allows Denver 311 staff to transfer inquiries to the appropriate partner agencies, as needed, to ensure timely resolution of citizen issues and questions. For example, requests that are received by Denver 311 can be routed to one of their partner agencies, such as the Department of Public Works, to respond to a pothole in the road. At the same time, its security measures limit access to certain information to a specified group of users, based on defined business needs.

Salesforce Selection Process

Salesforce was selected through a Request for Proposal (RFP) process, part of which required vendors to complete a Cloud Services RFP Technical Requirements Document (Document). The Document is divided into two sections to assess different provider capabilities.

- **Cloud Provider Security Risk Assessment** – The first section of the Document is used by Technology Services (TS) to assess the overall security risk of a cloud provider. TS uses criteria developed by the Cloud Security Alliance (CSA) called the Cloud Security Matrix (v3.0).[1] The CSA Cloud Security Matrix has 16 control domains that cover key areas such as application and interface security, audit assurance and compliance, data security and information lifecycle management, encryption and key management, and identity and access management.

[1] The CSA is a member-driven organization, chartered with promoting the use of best practices for providing security assurance within Cloud Computing, and providing education on the uses of Cloud Computing to help secure all other forms of computing. Cloud Security Alliance, accessed June 12, 2017, https://cloudsecurityalliance.org/about/.

- **Provider Compatibility** – The second section of the Document covers specific City controls, including end-user device compatibility.

Two members of TS executive management, both of whom have professional expertise in the areas of application and information security reviewed the RFP response that was submitted by Salesforce. TS subsequently selected Salesforce after reviewing and comparing it to other RFP responses submitted by other providers. The City and Salesforce then entered into a contract for services.

TS added a provision into the contract with Salesforce specifying that all City and end user data will be encrypted, both in transmission from Salesforce and in storage, to prevent unauthorized access. The contract also requires the completion of a System and Organization Controls 2 (SOC2) audit, or another mutually agreed upon audit, of Salesforce's security policies procedures and internal controls on an annual basis.

The City's Technology Services department reviewed Salesforce for data security capabilities and added a provision to the contract requiring encryption of end user data.

Salesforce Implementation

The Salesforce implementation process was primarily performed by an external vendor with assistance from a project manager from TS. Representatives from agencies that would be using Salesforce were involved in the implementation process to provide business requirements and perform user acceptance testing. The statement of work for the project required the following steps be finalized prior to project completion: planning, analysis, design, build, validation, deployment, training, documentation, and acceptance testing. Client sign off was noted as acceptance criteria for different stages of the project plan. The third-party vendor used its own project management software to archive project artifacts[2].

Implementation Included Steps to Assess Data Security Requirements – The data security and privacy requirements established through the initial RFP and the contract were addressed during the analysis, build, and validation phases, as follows:

- **Analysis Phase** – During the analysis phase, TS and the external vendor held meetings with user agencies to gain an understanding of their specific data and security requirements.
- **Build Phase** – The build phase established several security elements including organization-wide security, user profiles, and data sharing rules.
- **Validation Phase** – The validation phase included the creation of a test plan with test cases that were mapped to the business requirements including requirements for data privacy and security.

City Agencies That Use Salesforce

The initial Salesforce roll-out in 2015 implemented the system for use by Denver 311 and its partner agencies. A Denver 311 *partner agency* is defined as a City agency the 10-digit telephone number for which automatically rolls into the Denver 311 contact center when dialed by a customer. Information from these calls is then recorded in Salesforce. The system's CRM

[2] Artifacts are documents associated with an IT project, such as risk assessments, Gantt charts, test plans, and budgets.

functionality allows sharing of information between Denver 311 and its partner agencies, which include the following:

- City Council
- Department of Community Planning and Development, Neighborhood Inspection Services Division
- Department of Public Works, Transportation Division and Solid Waste Management Division
- Department of Environmental Health, Denver Animal Protection and Environmental Quality Division
- Department of Excise and Licenses
- Department of Finance, Treasury Division
- Denver Motor Vehicle
- Office of the Clerk and Recorder

Salesforce also provides a platform for custom applications for agencies that have their own internal call centers or support staff and allows those agencies to restrict access to their case data. The following agencies started using Salesforce in 2015 in capacities not related to partnering with Denver 311:

- Mayor's Office
- Office of Economic Development
- Department of Parks and Recreation
- Peak Academy
- Controller's Office, Payroll Division
- Denver International Airport
- Department of Human Services

A City employee working in an agency that has Salesforce may request access to the system by submitting a ticket through an application called ServiceNow. A user profile is then assigned based on the role in the Salesforce application and the role that the user requires to perform his or her job.

OBJECTIVE

The objective of the audit was to assess the potential for unauthorized user access to personally identifiable information (PII) in Salesforce.

SCOPE

The audit scope included Salesforce access controls, program management, and contractual agreements and included documents from 2014 through 2017. The audit did not include a complete review of all Salesforce Information Technology General Controls.

METHODOLOGY

We applied various methodologies during the audit process to gather and analyze information pertinent to the audit scope and to assist with developing and testing the audit objectives. The methodologies included the following:

- Conducting interviews with Technology Services staff
- Conducting interviews with the Department of Human Services and the Controller's Office personnel to gain an understanding of their agencies' Salesforce data security and privacy requirements
- Reviewing the business requirements documentation gathered for the initial Salesforce project management initiative
- Reviewing project documentation located in the ServiceNow Project and Project Intake modules
- Reviewing the contract for the Salesforce license and third-party implementation
- Executing Salesforce queries and evaluating results for PII based on continuous auditing

FINDING

Technology Services Should Improve the Management and Administration of Salesforce

In seeking a new customer relationship management (CRM) tool for the City and County of Denver (City), Technology Services (TS) performed a thorough evaluation of Salesforce to ensure that it could meet the City's security requirements for a vendor-hosted application. TS sought out personnel with extensive knowledge of the Salesforce CRM to provide in-house expertise in this process. However, the Auditor's Office recently discovered that the system allowed unauthorized access to personally identifiable information (PII) entered by a City agency that uses Salesforce to help meet its business objectives. Upon notification, TS took quick action to secure this sensitive information. Despite mitigating the risk in the short term, our audit identified additional opportunities for TS to improve its management and administration of Salesforce, including monitoring vendor performance and reporting to ensure that all contract terms are continually being met.

Auditors Found PII Data in Query Results Using a Denver 311 Supervisor Profile

While performing continuous auditing activities with Denver 311 contact center data, Auditor's Office personnel ran a Salesforce report using a Denver 311 Supervisor role provided by TS. Continuous auditing is a method used to identify risk areas in an efficient and timely manner. This auditing approach uses automated analysis of data fields to identify anomalies or outliers in the data. To analyze Denver 311 contact center data, Auditor's Office personnel created a set of key words that, if flagged in a dataset, could indicate a potential risk. If a citizen-initiated call to Denver 311 included one or more of the key words, the entry would be highlighted for further review. Through this process, we found entries in the Salesforce report that included PII. We then conducted a secondary query to identify other instances of PII entered into Salesforce, such as *SSN* (Social Security Number) and *SSAN* (Social Security Account Number), to assess the volume of PII that could be viewed by auditors using the Denver 311 Supervisor Salesforce profile.

After consulting with our information technology (IT) auditors and other Auditor's Office personnel, the data issues were communicated to the Mayor, TS, and other relevant parties in March 2017. The Auditor's Office and TS personnel collectively concluded that the report largely contained data from other Salesforce user agencies, and not primarily Denver 311 contact center data. Specifically, much of the data had been entered into Salesforce by the Department of Human Services (DHS) and the Controller's Office's Payroll Division. Due to the sensitive nature of PII, and the fact that it was accessed using a Denver 311 Supervisor profile, we concluded that the risk associated with this discovery warranted additional audit work.

DHS and the Payroll Division Informed TS That They Would Store PII Data in Salesforce

During the Salesforce implementation process, user agencies such as DHS and the Payroll Division submitted specific data security and privacy requirements for their data to the implementation vendor or TS to ensure that it would be protected once entered into Salesforce. Interviews with DHS and Payroll staff confirmed that these agencies intended to use the Salesforce application to securely store PII and other sensitive data and to limit access to that data to their own users. Descriptions of DHS security requirements that were gathered by the implementation vendor

support this assertion and include the following statements: "As DHS, I do not want other agencies to see DHS data on cases, contacts, or accounts" and "As DHS, I do not want to see data from other agencies regarding my constituents." After DHS was notified that other Salesforce users may have had access to some of their entries that contained PII, and until the situation could be remediated, DHS had to institute a revised business process. Since DHS is required to verify client identity using social security numbers as unique identifiers, DHS personnel revised their process by storing this information in another system until remediation efforts were completed and their data was secured from unauthorized access.

Security requirements for the Payroll Division were collected as well, but using a different method, since Payroll was not part of the initial Salesforce roll-out. When the Payroll Division requested Salesforce in 2015, they communicated their security and privacy requirements during the project intake process carried out by TS. The intake form specifically asks whether the request will include PII such as social security numbers, birth dates, health information, credit card or banking information, or safety records. The project intake form also requests information to help TS determine whether the data entered into the system will be shared with other agencies or applications. When we reviewed the project intake form completed by the Payroll Division to request Salesforce, we noted that the form indicated that the agency works with PII data that they would be entering into the system and that it did not need to be shared with any other agency or application.

Denver 311 Supervisor Profile Did Not Meet Privacy and Security Requirements

We found that the Denver 311 Supervisor profile in Salesforce had two settings that allowed the user of the profile to view all records within any City agency using Salesforce and to view all case data. With these settings in place, a user with the Denver 311 Supervisor profile could view or report on all data, including records belonging to DHS that should have been available only to other DHS users. DHS personnel were not aware that other users had potential access to the agency's data. Auditors subsequently determined that the Denver 311 Supervisor profile was also used as the model for two other Salesforce user profiles—Accounting Manager and Account Support Team—which received view-all-permissions to case data as well.

During the implementation of Salesforce, a user profile was created with broad permissions not intended by initial security specifications.

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. Industry best practices support this conclusion. Specifically, the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) discusses the concept of *least privilege,* which entails restricting access to sensitive data to only those individuals who must access the data to perform specified job duties. TS's Data Handling and Classification Policy includes the concept of least privilege, as well.

During our research, we obtained no evidence that would explain why the three problematic profiles were created with overriding access to data and cases. Many of the project management documents that would have been created during the Salesforce design and implementation process were not available upon request. It is possible that the profiles resulted from inadequate testing, but without relevant documentation, this possibility cannot be assessed. It is also possible that the documented DHS and Payroll Division security requirements were not communicated to all of the appropriate system

administrators during implementation. When the PII data belonging to DHS was first discovered by the Auditor's Office, one of the Salesforce administrators was unaware of DHS security and privacy requirements. Irrespective of the ultimate cause of the mistake, the inappropriate profile and security settings that resulted should have been documented and shared with Salesforce administrators to ensure that all members of the team are knowledgeable of the security requirements for each agency.

RECOMMENDATION 1.1

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

Agency Response: Agree, Implementation Date - Implemented

RECOMMENDATION 1.2

Technology Services should ensure that user profile security settings are documented and maintained for Salesforce administrators.

Agency Response: Agree, Implementation Date - Implemented

RECOMMENDATION 1.3

Technology Services should document information about Salesforce applications and specific security requirements for user agencies.

Agency Response: Agree, Implementation Date – March 31, 2018

Unauthorized Access within Salesforce Was Addressed

TS addressed the issue of unauthorized access prior to the completion of the audit work. Specifically, TS established a change management process that includes migrating relevant Salesforce code to the Salesforce test environment where it was tested by both TS personnel and agencies. According to TS, staff from DHS, the Payroll Division, and Denver 311 participated in the testing. Denver 311 testers were tasked with verifying that they could not see Payroll or DHS data while still retaining the access needed to work with their partner agencies, such as the Department of Public Works and Denver Animal Protection. Testers from the Payroll Division and DHS validated that they could see all cases and information as before. After user acceptance testing was completed, the changes were deployed to the production environment on May 3, 2017.

The Auditor's Office did not participate in this user acceptance testing, but reran the same Salesforce query seeking records containing *SSN* (Social Security Number) and *SSAN* (Social Security Account Number), after the deployment to the production environment. The resulting data set contained significantly fewer records. After analyzing the data, we concluded that the

Denver 311 Supervisor profile no longer had access to retrieve the DHS or Payroll Division records. The data set still contained three records that included full social security numbers; however, after further examination, we determined that these instances of PII were provided by citizens during submissions of information to Denver 311 using the City's pocketgov application. To eliminate this type of unnecessary disclosure of PII to unauthorized users, citizens should be reminded of the risks associated with providing PII when not required to do so.

RECOMMENDATION 1.4

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.

Agency Response: Agree, Implementation Date – March 31, 2018

Technology Services Has Not Fully Monitored Salesforce Security Documentation

Although TS personnel reviewed and approved the security policies and practices of Salesforce during the RFP process, they have not continued to verify that Salesforce is meeting these critical security practices. If Salesforce is not configured to meet accepted security standards, City data could be at risk of unauthorized access or loss.

As part of our audit work, we assessed what TS has done to ensure the ongoing security of the data housed in the Salesforce system. Although TS reviewed a System and Organization Controls 2 (SOC2) report for Salesforce during the RFP process, we found that TS has not subsequently received or reviewed attestation reports—such as a SOC2 report, vulnerability scan, or penetration test—for Salesforce, even though the contract for the Salesforce software license indicates that Salesforce should provide these reports on an annual basis.[3] A SOC 2 report provides information and assurance about an organization's controls around security, data confidentiality, integrity, and availability.[4] Vulnerability scan and penetration test results are also valuable in assessing the security posture of a cloud service provider. A vulnerability scan is a computer program that inspects an application, a computer, or a network for potential areas of weakness that could be exploited. A penetration test takes the assessment process further by attempting to break into a system using security weaknesses and then reporting the results to the appropriate management. The vulnerability scan and penetration test can be used by an organization to test

After the initial security review Technology Services has not subsequently reviewed SOC2 reports, vulnerability scans, or penetration tests to verify the ongoing security of the Salesforce platform.

[3] System and Organization Controls (SOC) reports are issued by an independent Certified Public Accountant. There are three types of SOC reports for service organizations: a SOC 1 report is a report on controls at a service organization relevant to user entities' internal control over financial reporting; a SOC 2 report is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy; and a SOC 3 report is a trust services report for service organizations.

[4] "SOC for Service Organizations: Information for Service Organizations," American Institute of CPAs, accessed March 7, 2016, http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganization'sManagement.aspx

its "security policy compliance, its employees' security awareness, and the organization's ability to identify and respond to security incidents."[5]

Further, the City's Executive Order 8, section A, contains City rules and requirements regarding contract compliance. It states that the initiating authority should monitor performance under the contract to ensure that the terms of the contract are met. However, TS is not adhering to Executive Order 8, or their own Salesforce contract, to ensure that Salesforce maintains security compliance. TS has an established process, documented in their Process – Vendor Attestation Review procedure for reviewing SOC reports. Specifically, the procedures states that SOC reports should be requested and reviewed for technology vendors providing services to TS.

As required by the contract, TS should request these reports and review them to confirm that Salesforce continues to meet the City's security and privacy requirements. Specifically, TS should ensure that any exceptions that have been noted in these reports are adequately addressed by Salesforce management. If TS becomes aware of any Salesforce issues, they can then monitor the issue through to resolution and implement mitigating controls, if necessary. Although TS hired a contract manager to ensure compliance with all TS contracts, this individual is still in the process of implementing a tool to manage and track required contract deliverables. However, if TS continues not to monitor Salesforce security practices, the City will be at risk for not safeguarding constituents' sensitive personal data. Therefore, to ensure that the contract manager adequately monitors Salesforce's security compliance, TS should obtain and review all required reports for Salesforce on an annual basis and confirm that the contract management and tracking tool is indeed implemented and working as intended.

RECOMMENDATION 1.5

Technology Services should obtain and review Salesforce SOC2 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.

Agency Response: Agree, Implementation Date – March 31, 2018

RECOMMENDATION 1.6

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.

Agency Response: Agree, Implementation Date – March 31, 2018

[5] "Pen test (penetration testing)" definition, Techtarget Network website, accessed May 31, 2017, http://searchsoftwarequality.techtarget.com/definition/penetration-testing.

RECOMMENDATIONS

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

Auditee Response: Agree, Implementation Date - Implemented

Auditee Narrative: *The Technology Services Project Management Office (PMO) has implemented a centralized repository for all project documentation. The PMO ensures that Salesforce project documentation and artifacts are stored in the centralized repository and are readily available.*

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

Auditee Response: Agree, Implementation Date - Implemented

Auditee Narrative: *Salesforce administrators can access the user roles and permission sets for our Salesforce instance via the administrative console.*

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

Auditee Response: Agency Response: Agree, Implementation Date – March 31, 2018

Auditee Narrative: *Technology Services will create a report in Salesforce to provide agencies with role definitions and user profile settings for periodic review.*

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.

Auditee Response: Agency Response: Agree, Implementation Date – March 31, 2018

Auditee Narrative: *Technology Services will update the language in the existing Privacy and Security Policy found on denvergov.org and pocketgov to discourage the submission of sensitive personal data. We will update this policy language not only on the Denver 311 webpage, but also the main Denvergov and pocketgov webpages. In addition, there is an Information Governance committee in place that is in the process of creating a comprehensive Protected Data Privacy Policy as part of an Executive Order.*

1.5 **Review Attestation Reports** — Technology Services should obtain and review Salesforce SOC2 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.

Auditee Response: Agency Response: Agree, Implementation Date – March 31, 2018

Auditee Narrative: *Per the contract requirements, Technology Services will annually obtain and review the Salesforce independent audit and security documentation to include the SOC2 report, vulnerability scans, and penetration testing results.*

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.

Auditee Response: Agency Response: Agree, Implementation Date – March 31, 2018

Auditee Narrative: *Technology Services will implement a contract module in Salesforce for comprehensive contract management including insurance renewals and attestation reports.*

AGENCY RESPONSE

Technology Services
201 West Colfax Avenue
Department 301
Denver, CO 80202

July 12, 2017

Auditor Timothy O'Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O'Brien,

The Office of the Auditor has conducted an audit of Personally Identifiable Information in Salesforce.

This memorandum provides a written response for each reportable condition noted in the Auditor's Report final draft that was sent to us on June 21, 2017. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
Technology Services Should Improve the Management and Administration of Salesforce

RECOMMENDATION 1.1 The Technology Services Project Management Office should ensure that Salesforce project documentation and artifacts are archived and readily available.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	Implemented	Andrea Denis 720-913-4810

Narrative for Recommendation 1.1
The Technology Services Project Management Office (PMO) has implemented a centralized repository for all project documentation. The PMO ensures that Salesforce project documentation and artifacts are stored in the centralized repository and are readily available.

RECOMMENDATION 1.2 Technology Services should ensure that user profile security settings are documented and maintained for Salesforce administrators.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	Implemented	Chad Mitchell 720-913-4953

Narrative for Recommendation 1.2
Salesforce administrators can access the user roles and permission sets for our Salesforce instance via the administrative console.

RECOMMENDATION 1.3 Technology Services should document information about Salesforce applications and specific security requirements for user agencies.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2018	Chad Mitchell 720-913-4953

Narrative for Recommendation 1.3
Technology Services will create a report in Salesforce to provide agencies with role definitions and user profile settings for periodic review.

RECOMMENDATION 1.4 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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2018	Jenny Schiavone 720-913-4881

Narrative for Recommendation 1.4

Technology Services will update the language in the existing Privacy and Security Policy found on denvergov.org and pocketgov to discourage the submission of sensitive personal data. We will update this policy language not only on the Denver 311 webpage, but also the main Denvergov and pocketgov webpages. In addition, there is an Information Governance committee in place that is in the process of creating a comprehensive Protected Data Privacy Policy as part of an Executive Order.

RECOMMENDATION 1.5 Technology Services should obtain and review Salesforce SOC2 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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2018	Tricia Scherer 720-913-4869

Narrative for Recommendation 1.5
Per the contract requirements, Technology Services will annually obtain and review the Salesforce independent audit and security documentation to include the SOC2 report, vulnerability scans, and penetration testing results.

RECOMMENDATION 1.6 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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2018	Chad Mitchell 720-913-4953

Narrative for Recommendation 1.6
Technology Services will implement a contract module in Salesforce for comprehensive contract management including insurance renewals and attestation reports.

Please contact Tricia Scherer at 720-913-4869 with any questions.

Sincerely,

Scott Cardenas
Chief Information Officer

cc: Valerie Walling, Deputy Auditor, CPA, CMC
Katja E. V. Freeman, Audit Manager, MA, MELP
Christine Binnicker, Deputy Chief Information Officer
Chris Todd, Chief Technology Officer