CITY AUDITOR'S OFFICE

ActiveNet Application Controls

May 9, 2019

AUDIT REPORT NO. 1904

May 9, 2019

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *ActiveNet Application Controls*, which was included on the Council-approved FY 2018/19 Audit Plan as a contracted information technology audit. We contracted with Myers and Stauffer LC, to conduct an application controls audit of the ActiveNet system, which is a cloud-based recreation management software used primarily by the City's Community Services Division for membership management, program/class registration and scheduling, facility reservations and cashiering.

Overall, auditors found that ActiveNet application controls were reasonably designed and implemented. However, opportunities to increase the maturity of these controls include establishing policies and procedures to strengthen account management practices and handling of personally identifiable information. Additionally, improvements could be made to vendor management and monitoring practices, such as ensuring security compliance reports and activity logs or reports are requested and reviewed.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Lai Cluff, CIA – Sr. Auditor

TABLE OF CONTENTS

AUDIT HIGHLIGHTS

ActiveNet Application Controls

May 9, 2019 Audit Report No. 1904

WHY WE DID THIS AUDIT

This audit of ActiveNet Application Controls was included on the City Council-approved fiscal year (FY) 2018/19 Audit Plan as a contracted information technology (IT) audit. The City Auditor's Office contracted with IT audit specialists from Myers & Stauffer LC to conduct this audit to evaluate the effectiveness of ActiveNet application controls, including management of its cloud-related risks.

BACKGROUND

ActiveNet is a recreation management software system used for cashiering, facility reservations, membership management, program/class registration and scheduling, and transaction accounting. It is used by Parks & Recreation, Preserve, Human Services, Library, and Human Resources departments. The Community Services Technology Group (CSTG) staff manages the software contract, serves as system administrators, and provides user support.

ActiveNet is a Software-as-a-Service application. The vendor, Active Network LLC, is responsible for storing and securing the City's data and processing payment card transactions. City staff log in using a web-based portal. Customers can also log in online to create accounts, register for activities and pay fees.

City Auditor's Office

City Auditor 480 312-7867
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

Overall, application controls were reasonably designed and implemented; however, stronger account management practices would help ensure appropriate user account access.

Policies and procedures should be expanded upon and formalized to:

- Ensure documented permissions guidelines are kept up-to-date
- Ensure required training has been completed and access-levels requested are consistent with documented permissions guidelines
- Ensure generic and stale user accounts are reviewed
- Establish policies for off-site/remote use of the application

Additionally, access removal was not requested timely for 3 of 16 deactivations reviewed and was not requested at all for another 4 former employees.

Policies and training are needed to protect personally identifiable information (PII).

CSTG has not identified the data in ActiveNet that contains customer PII and ActiveNet users have not received relevant training.

Vendor management and monitoring practices could be improved.

Vendor security compliance reporting requirements have not been regularly monitored and enforced. Additional activity reports are needed.

Other operational areas for improvement.

System controls requiring supervisor approval of refunds can be activated, incident response plans are not formalized, and data loss prevention monitoring is needed.

WHAT WE RECOMMEND

We recommended the Community Services Division:

- Strengthen policies and procedures relating to account management.
- Work with IT to establish PII policies, protection and training.
- Monitor vendor security compliance reports and obtain additional activity and fee monitoring reports.

MANAGEMENT RESPONSE

The department agreed, and CSTG will be working with the department's subject matter experts and the City's Information Technology department on improvements.

BACKGROUND

This audit of *ActiveNet Application Controls* was included on the City Council-approved fiscal year (FY) 2018/19 Audit Plan as a contracted information technology (IT) audit. We contracted with Myers & Stauffer LC, to evaluate the ActiveNet application controls.

ActiveNet is a recreation management software system used for Point-of-Sale (POS) cashiering, facility reservations, membership management, program/class registration and scheduling, and transaction accounting. The Community Services Division primarily uses the system in its Parks & Recreation, Preserve, Human Services, and Library departments. As well, the Human Resources department uses ActiveNet as a POS for City Store transactions. The Community Services Technology Group (CSTG) staff manages the software contract, serves as system administrators, and provides user support.

FY 2017/18 Activity

Programs/Classes	3,025
Online Enrollments	26,564
Total Enrollments	41,981
Facility Rentals	32,440

SOURCE: Auditor analysis of ActiveNet data for activity enrollments and facility rentals.

The Division began using ActiveNet in February 2016 when Active Network LLC, the vendor, was no longer supporting the previous CLASS system. While the previous system was hosted on-premise, with data stored on City servers and managed by City staff, ActiveNet is a Software-as-a-Service (SaaS) application. The ActiveNet software is cloud-based, so staff log in using a web-based portal. The vendor is responsible for storing and securing the City's data and processing payment card transactions. As well, customers can log in online to create account credentials, register for activities and pay fees. Table 1 shows example transaction types processed by the various departments along with FY 2017/18 transaction totals.

Table 1. ActiveNet Receipts During FY 2017/18, by Department

Department	Example Transaction Types	Total (rounded)
Parks & Recreation	Program fees; admission fees for pools, fields, fitness centers, courts, and events; facility/equipment rentals; beer permits	$4,520,000
Library	Library fines, Library Store sales, printer/copier sales, facility rentals	490,000
Human Services	Youth & Family Services program fees, facility rentals, Senior Center program fees	360,000
Preserve	Commercial use fees	40,000
Human Resources	City Store sales	7,000
	Total	**$5,417,000**

SOURCE: Auditor analysis of ActiveNet Cash Receipts Export report for FY 2017/18.

ActiveNet Contract Fees

Rather than having a fixed software license cost and annual maintenance fees, ActiveNet's fee is variable based on the transaction type processed. As summarized in Table 2, the City pays a base 1.5% transaction fee for cash or check transactions and 4.25% (an additional 2.75%) for credit or debit card transactions. Online payment card transactions incur a minimum of $1.00 fee. Additionally, the contract provides a $0.10 flat fee for any credit card refunds that are processed.

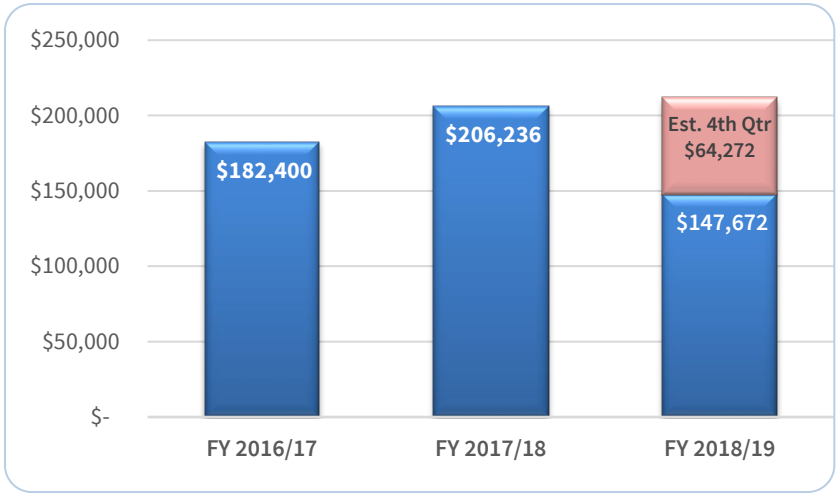
Table 2. ActiveNet Transaction Processing Fees

	Transaction Processing Fees
Cash or Check	1.50%
Credit/Debit Card	4.25%
Online Credit/Debit Card	4.25%, $1.00 minimum
Cash/Check Refund	n/a
Credit/Debit Refund	$0.10

SOURCE: City contract #15SS014 *City Services – Non-RFP Software as a Service Contract* (ActiveNet).

ActiveNet deducts its transaction fees before depositing the balance into the City's bank account each day. As shown in Figure 1, ActiveNet's FY 2017/18 fee totaled more than $206,000.

Figure 1. ActiveNet Fees by Fiscal Year



Note: 4th Quarter of FY 2018/19 was estimated using average fees for the same quarter in the prior 2 years.

SOURCE: Auditor analysis of accounting entries for ActiveNet fees.

Application Controls

Application controls are a subset of internal controls that relate to an application system and the information managed by that application. Application controls consist of the manual and automated activities that help achieve the business objectives of timely, accurate and reliable information. Criteria for application controls include effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

The vendor is responsible for the application's computing environment, which would include a secure physical facility, securing data at rest and in transit, and for ensuring that the application, databases, updates and operating systems meet industry standards and legal requirements. As well, because ActiveNet processes credit and debit cards, it must also comply with the Payment Card Industry Data Security Standard (PCI DSS).

> "Contractor assumes all responsibility for the computing environment supporting the hosted applications and ensuring the applications, databases, updates, and operating systems meet industry standards and applicable federal and state laws."
>
> **SOURCE**: COS contract # 15SS014

OBJECTIVES, SCOPE, AND METHODOLOGY

This audit of *ActiveNet Application Controls* was included on the City Council-approved fiscal year (FY) 2018/19 Audit Plan as a contracted information technology (IT) audit to evaluate a selected information system, operational area or contract. We selected the ActiveNet information system for review. The audit objective was to evaluate the effectiveness of ActiveNet application controls, including management of its cloud-related risks.

We contracted with Myers & Stauffer LC as IT audit specialists to conduct the audit of ActiveNet application controls. As required by *Government Auditing Standards*, we evaluated the qualifications and independence of the specialists and documented the nature and scope of the specialists' work, including the objectives and scope of work, intended use of the specialists' work to support the audit objectives, and the specialists' procedures and findings.

To gain an understanding of the ActiveNet system, the audit specialists reviewed:

- ActiveNet contract (#15SS014 City Services – Non-RFP Software as a Service Contract)
- Audit Report No. *1311, Selected Application Controls over the City's CLASS System,* issued June 2013 by the City Auditor's Office

Auditors also interviewed the Community Services Technology Group (CSTG) and system users from the Library Systems and Parks & Recreation (leisure education and facility booking group, recreation center, and after-school programs). As well, the Business Operations Manager and Sr. Management Analyst in Community Services and an Accountant from the City Treasurer's Office were interviewed to gain an understanding of the financial data and reconciliation process for ActiveNet financial transactions.

To meet the audit objectives, auditors performed the following procedures:

- Reviewed and assessed policies and procedures and roles and responsibilities related to ActiveNet application controls.
- Evaluated logical access controls, including verifying password requirements and user authorization and deactivation processes.
- Reviewed segregation of duties controls, including sampling refund documentation and reviewing for manual approvals.
- Assessed controls for system authentication and authorization, including granting, modification, revocation, and periodic revalidation of access, and access privileges for individuals to the system.
- Reviewed processes and procedures for monitoring and logging application access and processes and procedures for reviewing log information.
- Tested samples of user accounts to determine whether system access and permissions were appropriately authorized and users were current employees or contractors.
- Reviewed contract administration and oversight of the cloud services vendor; requested and reviewed security compliance reports required by the contract.
- Reviewed and tested ActiveNet application edit and audit controls.

Most application controls testing was conducted in the training database, a copy of the live database used for testing and training purposes.

The audit specialists used best practices and standards from the National Institute of Standards and Technology (NIST) to evaluate ActiveNet controls. Specifically, NIST Special Publication 800-53 was applied to evaluate security and privacy controls.

Overall, auditors found that ActiveNet application controls were reasonably designed and implemented. However, auditors identified opportunities for improvement to increase the maturity of the IT-related controls. These include establishing policies and procedures to strengthen account management practices and handling of personally identifiable information. As well, vendor management and monitoring practices could be improved.

We conducted this performance audit 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. Audit work took place from January to March 2019.

FINDINGS AND ANALYSIS

1. Overall, application controls were reasonably designed and implemented; however, stronger account management practices would help ensure appropriate user account access.

Account management controls include requiring supervisory or management approval to create information system accounts and monitoring account use. Since our 2013 audit of the division's CLASS system, the Community Services Technology Group (CSTG) staff has improved its information technology controls, including documenting user profiles and role-based account permissions, establishing a work order system to document and track requests to add or remove user access, and incorporating an annual review of authorized users. However, existing policies and procedures need to be expanded upon to help ensure access is appropriately authorized. As well, procedures for removing access for terminated employees need clarification.

A. Policies and procedures regarding system access control should be expanded upon and formalized.

Existing CSTG account administration policies do not adequately address ActiveNet access approval and the use of role-based security groups. The department implemented a work order process to document and track system access requests, and the policy requires that supervisors create the work order or receive a copy of it. However, the policy could be expanded upon to cover the following areas:

1. System permissions did not always align with documented permissions. To ensure appropriate separation of duties, CSTG developed an *ActiveNet Permissions User Profile Function Authorities Matrix* with stakeholder input. The matrix documents the user profiles and role-based access levels based on various positions. However, for each of the 12 user profiles auditors reviewed, the actual permissions granted in ActiveNet did not align with those described in the matrix. Division policies currently do not direct supervisors to review the specific permissions and ensure that they are consistent with profiles established in the matrix when requesting and approving access for employees.

2. Approval of new users and the annual review of user accounts are not consistently documented. Seven of the 25 sampled user accounts were not included in CSTG's most recent annual review of user access completed in August 2018. Further, 3 of these 7 did not have evidence of the initial user access approval.

3. Required training is not verified prior to authorizing new users. While cash handling and PCI compliance training are required for cash handlers, the existing policies and procedures do not require supervisors to confirm that required training has been completed before submitting requests for new user access. Eleven of 25 users reviewed had not completed the required annual PCI compliance training. Based on the user profiles, these users had cashiering privileges allowing them to handle payment transactions.

4. Generic accounts have not been reviewed. Auditors noted 7 generic system accounts within ActiveNet. Generic accounts are not assigned to an individual and are generally created for a specific purpose; the account's access privileges should be limited to that purpose. CSTG created two of the 7 accounts, one for scanning functionality and the other as a test

account. But CSTG does not know the purpose or the access privileges of the other 5 generic accounts.

5. Stale accounts should be deactivated. ActiveNet was not configured to identify and report on accounts that have not been accessed for a defined period of time, such as 90 days. Allowing stale accounts to retain access increases the risk of unauthorized activity occurring through an unused account. After being made aware of this issue during the audit, CSTG enabled a system option that results in automatic expiration for accounts after 90 days of inactivity.

6. There are no policies governing off-site (remote) ActiveNet use. As a cloud-based application, ActiveNet is available from any device with internet access. As well, system users can modify the workstation setting to process transactions through a different workstation than the one they are physically using. This increases the risk of error and the potential for unauthorized transactions and access to data.

B. System access was not timely removed for some terminated employees.

CSTG removes a terminated employee's ActiveNet access when department staff submit a work order for the deactivation.

1. Auditors reviewed a sample of 24 calendar year 2018 work orders requesting account deactivation:

   - For 5 of the 24, the account had not been appropriately deactivated by selecting the "Prevent Further Use" option.
   - For 16 of the 24, CSTG closed the work orders more than 10 days after the employee's last date worked. However, for 3 of the 16, the supervisor submitted the work order more than 100 days after the employee's last date worked. According to management, these supervisors may have delayed the termination process for employees who were expected to potentially return to city employment.

2. Auditors also compared ActiveNet authorized users to a Human Resources (HR) report on calendar year 2018 terminations. This comparison identified 4 additional user accounts that had not been deactivated and work orders had not been submitted to deactivate them. Three of these 4 had been active for more than 100 days after the employee's separation. For these instances, the typical resignation processes were not applicable, and department staff did not submit a work order for CSTG to deactivate the accounts. When terminations happen without prior notice, HR typically notifies the City's IT department and Municipal Security. However, the City IT department revoking network access does not prevent active users from accessing the ActiveNet system.

For SaaS applications such as ActiveNet, timely removal of user access is critical since an authorized user can access the application from any device with internet access.

Recommendations:

The Community Services Division should:

A. Expand the current policies and procedures to require supervisors to justify departures from the matrix and ensure training is provided before account access is authorized. Further, CSTG should document reviews of all user accounts, including generic accounts, and require

supervisory approval before reinstating a stale account. As well, the division should develop an ActiveNet remote access policy limiting access to authorized uses.

B. Remind department staff to timely notify CSTG to remove ActiveNet access for every employee termination, even those where an employee may potentially return to City employment in the future.

2. Policies and training are needed to protect personally identifiable information.

The National Institute of Standards and Technology (NIST) defines personally identifiable information (PII) as *"any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."* Some PII is more sensitive and requires stricter handling guidelines as it could substantially harm an individual if lost, compromised or disclosed without authorization. Examples of PII and sensitive PII are shown below.

PII	Sensitive PII
Name	Social Security Number
Home Address	Driver's License Number
Phone Number	Financial Account Number
Email	Biometric Identifiers

SOURCE: U.S. Department of Homeland Security *Handbook for Safeguarding Sensitive Personally Identifiable Information*

The City has not established a data classification policy to identify PII or developed PII policies and training for staff. Community Services has not updated its Essential Records Listings to reflect ActiveNet data as the replacement for CLASS.

A. The City IT department has not yet established citywide policies regarding the classification and handling of PII, and CSTG has not specifically identified the ActiveNet fields containing PII or sensitive PII. ActiveNet maintains customer personally identifiable information that may also include sensitive PII.

   As well, PII-related training has not been provided to staff using ActiveNet. For example, there are currently no formal procedures to verify an ActiveNet customer's identity before updating or sharing customer information that is already in the system. Additionally, sensitive PII, such as driver's license numbers obtained for beer permits, should be better secured in the system.

B. Since the transition from CLASS to ActiveNet in 2016, Community Services has not updated its Essential Records Listing. The Essential Records Listing is used to identify critical records for continuing operations in the event of an emergency or disaster. Currently, this list identifies the CLASS database records, which were stored on City servers and managed by the IT department. By contract, Active Network is responsible for the City's ActiveNet transaction data storage, backups, and retention.

The ActiveNet contract requires the vendor to store and retain data for the length of time specified by the City and return any stored data upon the termination of the contract. The specified retention period should be based on the City's records retention requirements.

Recommendations:

The Community Services Division should:

A. Work with City IT to develop a formal policy regarding the classification and handling of PII. Any ActiveNet fields containing PII should be identified and training should be provided to staff regarding the handling of customer PII.

B. Update the Essential Records Listing with ActiveNet information.

3. Vendor management and monitoring practices could be improved.

Monitoring of vendor compliance with security requirements is critical for systems where the City relies on the vendor to store and process transaction data. The audit found that security compliance reports were not being regularly reviewed and additional activity logging reports should be requested and reviewed periodically. As well, the Division has not reviewed ActiveNet fees for compliance with the contract.

A. Vendor security compliance reports need more active and consistent monitoring.

The ActiveNet contract requires the vendor to provide any current "SSAE 16 audit report, or its replacement audit report" upon request. Additionally, the ActiveNet contract requires the vendor to provide an attestation that the vendor's application has been tested for common security vulnerabilities and meets the standards described in the "OWASP Top 10."[1]

CSTG had not been regularly requesting and reviewing these security compliance reports. When requested during the audit, the vendor was unable to provide documentation of the OWASP Top 10 security vulnerabilities testing. As well, the Statement on Standards for Attestation Engagements No. 18 (SSAE 18, the replacement for SSAE 16) report provided by the vendor was not completed by a CPA in accordance with the standards. The vendor provided a PCI compliance report and no issues were noted.

B. ActiveNet provides CSTG with limited reporting capabilities for monitoring system activities, such as changes to user account profiles and privileges, system configuration, fee tables and those made by Active Network personnel or activity occurring outside of normal business hours. According to CSTG, Active Network will provide additional system activity logs upon specific request. Obtaining and reviewing these reports on a regular basis could help identify any potential security or data issues.

C. The division does not verify the vendor's compliance with contract fees, and ActiveNet's current Agency Fee reports do not provide sufficient information to allow verification.

[1] The Open Web Application Security Project (OWASP) is non-profit organization dedicated to web application security. The OWASP Top 10 identifies the top 10 most critical web application security risks. The list is regularly updated for changes in the security environment.

Active Network charges fees on each financial transaction processed through ActiveNet as described in the Background on page 4. The vendor then retains its fees from payment card proceeds before depositing the balance to the City's bank account.

The Accounting department verifies that the fee amounts actually withheld from the deposit matches the Agency Fee reports. However, Community Services has not compared this fee calculation to the contractually provided fees. Further, the ActiveNet Agency Fee reports do not show all relevant information needed to verify the fee calculations. As well, the more detailed Agency Fee Report showed incorrect fee amounts on customer transactions that had multiple payment types. Our estimates of FY 2017/18 fees indicate that any differences would be minor; however, Active Network should be providing sufficient details to allow fee verification.

Recommendations:

The Community Services Division should:

A. Regularly request and review contract-required security compliance reports to ensure the vendor is maintaining effective security controls.

B. Work with Active Network to obtain activity logging reports on a continuous basis and establish a process for monitoring changes and unusual activity.

C. Work with Active Network to create a report that will assist the division in verifying compliance with contractual fees.

4. Other operational areas for improvement.

Auditors' review of application controls identified a few other areas for improvement. Management should consider enabling system controls requiring supervisor approval of refunds over pre-determined amounts, department incident response plans should be formalized, and technical solutions for data loss prevention should be considered.

A. Enabling system controls requiring supervisor approval of refunds may help minimize the risk of improper transactions. Refunds totaled about $286,000 during FY 2017/18. This audit sampled 25 refunds for review and found that 2 of the 25 had insufficiently documented approvals. Past cash handling audits have also reported inconsistencies in supervisory review of refunds.

   All system users with cashiering privileges also have privileges to process refund transactions within ActiveNet. The division requires supervisors to manually review and sign refund documentation. While the ActiveNet application has an option to require supervisor electronic approval for refunds, this option has not been enabled. According to CSTG, management decided during system implementation that enabling this feature would potentially result in customer inconvenience.

   To lessen the customer inconvenience, however, the ActiveNet system control also allows management to set a refund amount, such as $20, for requiring the electronic supervisory approval. ActiveNet refund reports indicate that most refunds are small dollar amounts, but the larger refunds account for a significantly larger portion of the refund total. Specifically, as

shown in Figure 2, only 30% of refunds are greater than $60, but they account for more than 70% of total refunds. Enforcing supervisor approvals through ActiveNet could reduce the risk of unauthorized refunds.

Figure 2. FY 2017/18 ActiveNet Refunds

SOURCE: Auditor analysis of ActiveNet Refund Export report for FY 2017/18.

B. Formalizing incident response plans would reduce the risk of delays when issues arise.

   CSTG has informally designated incident response team members and provided ActiveNet users with guidance for contacting the CS Help Desk during certain events, such as application outages. However, CSTG policies and procedures lack specific protocol for handling incidents. Additionally, CSTG had not obtained guidance from City IT on what constitutes an incident and who to contact if an incident is identified.

C. Technical solutions are recommended for data loss prevention.

   Auditors also noted that technical solutions have not been implemented to monitor for potential data exfiltration or other disclosure events. These solutions may include programs that generate alerts for suspected data exfiltration, such as emailing sensitive information or large attachments and use of non-approved USB flash drives.

Recommendations:

The Community Services Division should:

A. Consider enabling system controls requiring supervisor approval of refunds, including setting a minimum refund amount for requiring supervisor approval.

B. Formalize incident response plans.

C. Work with City IT to explore technical solutions for data loss prevention.

MANAGEMENT ACTION PLAN

1. Overall, application controls were reasonably designed and implemented; however, stronger account management practices would help ensure appropriate user account access.

Recommendations:

The Community Services Division should:

A. Expand the current policies and procedures to require supervisors to justify departures from the matrix and ensure training is provided before account access is authorized. Further, CSTG should document reviews of all user accounts, including generic accounts, and require supervisory approval before reinstating a stale account. As well, the division should develop an ActiveNet remote access policy limiting access to authorized uses.

B. Remind department staff to timely notify CSTG to remove ActiveNet access for every employee termination, even those where an employee may potentially return to City employment in the future.

MANAGEMENT RESPONSE: Agree.

PROPOSED RESOLUTION:

A. CSTG will:
    1. Include updating the 'Active Network Permissions User Profile Function Authorities Matrix' as part of any updates to user profile groups.
    2. Update their existing process to document reviews of user accounts to ensure all user accounts are included.
    3. Update their existing account administration operating procedures to ensure stale accounts require supervisory approval before reinstating.
    4. Work with City IT to develop a remote access policy.

B. CSTG will work with division SP3, HR and City IT to identify where CSTG can be notified of employee departures.

RESPONSIBLE PARTY: CSTG, SP3, HR and City IT

COMPLETED BY: 11/1/2019

2. Policies and training are needed to protect personally identifiable information.

Recommendations:

The Community Services Division should:

A. Work with City IT to develop a formal policy regarding the classification and handling of PII. Any ActiveNet fields containing PII should be identified and training should be provided to staff regarding the handling of customer PII.

B. Update the Essential Records Listing with ActiveNet information.

MANAGEMENT RESPONSE: Agree.

PROPOSED RESOLUTION:

A. CSTG will work with City IT to develop a formal policy regarding the classification and handling of PII. Any Active Network fields containing PII will be identified and training will be provided to staff regarding the handling of customer PII.

B. CSTG will work with City IT and Community Services records manager to ensure Essential Records Listing are updated.

RESPONSIBLE PARTY: CSTG, Community Services and City IT

COMPLETED BY: 6/30/2020

3. Vendor management and monitoring practices could be improved.

Recommendations:

The Community Services Division should:

A. Regularly request and review contract-required security compliance reports to ensure the vendor is maintaining effective security controls.

B. Work with Active Network to obtain activity logging reports on a continuous basis and establish a process for monitoring changes and unusual activity.

C. Work with Active Network to create a report that will assist the division in verifying compliance with contractual fees.

MANAGEMENT RESPONSE: Agree.

PROPOSED RESOLUTION:

A. CSTG will Develop and implement a process of requesting and reviewing Active Network contract required security compliance reports.

B. CSTG will work with Active Network to obtain activity logging reports. CSTG will Develop and implement a schedule to review activity logs for irregularities or potential issues.

C. CSTG will work with Active Network to identify or create a report that will assist the division in verifying compliance with contractual fees.

RESPONSIBLE PARTY: CSTG

COMPLETED BY: 6/30/2020

4. Other operational areas for improvement.

Recommendations:

The Community Services Division should:

A. Consider enabling system controls requiring supervisor approval of refunds, including setting a minimum refund amount for requiring supervisor approval.

B. Formalize incident response plans.

C. Work with City IT to explore technical solutions for data loss prevention.

MANAGEMENT RESPONSE: Agree.

PROPOSED RESOLUTION:

A. CSTG will work with Subject Matter Experts to evaluate and review enabling system controls requiring supervisor approval of refunds.

B. CSTG will formalize incident response plans.

C. CSTG will work with City IT to explore technical solutions for data loss prevention.

RESPONSIBLE PARTY: CSTG, Subject Matter Experts and City IT

COMPLETED BY: 6/30/2020

City Auditor's Office
7447 E. Indian School Rd., Suite 205
Scottsdale, Arizona 85251

OFFICE (480) 312-7756
INTEGRITY LINE (480) 312-8348

www.ScottsdaleAZ.gov/auditor

City Auditor's Office
Kyla Anderson, Senior Auditor
Paul Christiansen, Senior Auditor
Lai Cluff, Senior Auditor
Cathleen Davis, Senior Auditor
Brad Hubert, Senior Auditor
Sharron Walker, City Auditor

The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability and integrity.