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.