AUDIT HIGHLIGHTS

ActiveNet Application Controls

May 9, 2019

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.