Vendor Access Controls Audit

March 6, 2020

Mayor

Betsy Price

Council Members

Carlos Flores, District 2
Brian Byrd, District 3††
Cary Moon, District 4†
Gyna Bivens, District 5
Jungus Jordan, District 6††
Dennis Shingleton, District 7††
Kelly Allen Gray, District 8
Ann Zadeh, District 9

† Audit Committee Chair
†† Audit Committee Member

City of Fort Worth
Department of Internal Audit
200 Texas Street
Fort Worth, Texas 76102

Audit Staff

Patrice Randle, City Auditor
John Riggs, Assistant City Auditor
Tom Wilson, IT Auditor

The Vendor Access Controls Audit was conducted as part of the Department of Internal Audit's Fiscal Year 2019 Annual Audit Plan.

Audit Objective

The objective of this audit was to evaluate the adequacy of security controls over vendor access to City of Fort Worth systems and data.

Audit Scope

Our audit covered active City of Fort Worth network accounts assigned to vendors and volunteers, as well as system access granted to those network accounts during FY2017 and FY2018.

Opportunities for Improvement

Improved management of vendor and volunteer access to the City's network

Discontinued use of generic City of Fort Worth network accounts

Improved access management of the ActiveNet system

Executive Summary

As a part of our FY2019 Annual Audit Plan, the Department of Internal Audit conducted a Vendor Access Controls Audit.

We identified 233 active City of Fort Worth (CFW) network accounts that had not been used since the accounts were created. Although unused, five of the accounts were listed as having taken the CFW's security training course.

Three generic CFW network accounts were used to access the City's network in July 2019. These accounts were not assigned to specific individuals.

A total of 65 ActiveNet system user accounts was assigned to individuals no longer employed with the CFW. We also identified 95 accounts that were assigned to ActiveNetwork LLC employees, 29 of which had financial administration user rights, meaning they had the ability to modify accounting information, adjust customer account balances and modify customer payment plans.

These findings are discussed in further detail, within the Detailed Audit Findings section of this report.

Table of Contents

Background

The City of Fort Worth (CFW) utilizes an extensive computer network as part of its daily operations. The network encompasses approximately 240 buildings, across roughly 1,200 square miles. The network connects over 9,000 devices (desktop/laptop computers, printers and mobile data computers), and provides access to approximately 7,000 employees and contractors/volunteers.

User access to the CFW's computer network and its related systems requires the use of a network account. Each network user account, created by the City's Information Technology Solutions Department (ITS), consists of a unique username and password. The rights and permissions, configured for each user account, correspond to each network account holder's individual job responsibilities.

Network accounts created for vendors contain rights and permissions based on contract terms, conditions, and statements of work. According to ITS personnel, any contract with associated information technology (IT) related services (where vendors will receive access to City networks) must include a Network Access Agreement that details the terms and conditions for network access. In addition, the sponsoring department must provide a Vendor/Contractor VPN Access Request Form to ITS.

Access rights and permissions granted to volunteers with a City network account are based on the specific business needs of a department. A signed, volunteer access acknowledgement form is required before a volunteer receives access to the network.

Volunteer accounts expire one year after activation, and must be renewed annually by ITS. Vendor accounts expire the earliest of one year after activation or the end of the contract term. ITS verifies that the vendor contract is in effect before reactivating associated accounts. Unless renewed, expired accounts are periodically purged by ITS personnel. A written departmental request is required to reactivate an expired network account.

Users may access the CFW's computer network and related systems by using a:

- CFW network-connected computer located at a City facility (on-site access);
- CFW network computer or server from a remote location (remote access); and/or,
- Virtual Private Network (VPN). VPN is an encrypted connection, over the internet, from an outside computer to a specific location/resource on the City's network.

Objective

The objective of this audit was to evaluate the adequacy of security controls over vendor access to CFW systems and data.

Scope

Our audit covered active CFW network accounts assigned to vendors and volunteers, as well as system access granted to those network accounts during FY2017 and FY2018.

Methodology

To achieve the audit objective, the Department of Internal Audit performed the following:

- interviewed personnel within the Information Technology Solutions Department;
- identified and reviewed vendor contracts executed during FY2017 and FY2018;
- identified and reviewed CFW computer software systems in use and accessible to vendors and volunteers;
- identified and reviewed CFW system/data access methods and rights made available to vendors and volunteers;
- identified and reviewed policies and procedures associated with granting, revoking, and monitoring CFW systems/data access granted to vendors and volunteers; and,
- evaluated internal controls related to CFW network access management for vendors and volunteers.

We conducted this 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 objective.

Audit Results

The Department of Internal Audit determined that ITS has a process for granting, renewing and revoking network access of vendors and volunteers. However, we identified user accounts that had not been used for an extended period, generic accounts, and user accounts assigned to individuals no longer employed with the CFW.

Internal Audit reviewed 531 CFW network accounts assigned to vendors and volunteers, and concluded that 233 of those accounts had not been accessed since the accounts were created. Five network accounts appeared on the CFW's 2019 security awareness training summary as having taken the security training. However, those network accounts had never been used.

Vendor personnel are required to be listed on a Vendor/Contractor VPN Access Request Form and volunteers must complete a volunteer access acknowledgement form prior to receiving access to the City's network. During our audit testing, we reviewed 57 CFW vendor and volunteer accounts. Internal Audit could not locate forms for 28 of those 57 accounts. ITS staff stated that copies of the forms are stored as attachments to ITS Help Desk tickets; however, separate copies of those forms are not retained for future reference. We also identified three generic network accounts used within the Police Department.

Internal Audit reviewed ActiveNet system user accounts, and compared those accounts to a complete list of CFW network users. The review showed that 65 ActiveNet user accounts were active for individuals no longer employed with the CFW. In addition, 95 accounts were identified as belonging to ActiveNetwork LLC employees, 29 of which had financial administration user rights with the ability to modify ActiveNet general ledger accounts, customer account balances and payment plans, and accounting journal entries.

Internal Audit also identified 11 active FASTER fleet management system user accounts belonging to former employees. In addition, two users had the same system operator ID, and two users had more than one assigned system operator ID. There were 71 employees and one contractor with the ability to reopen closed work orders. Since the FASTER fleet management system was upgraded to a web-based version in December 2019 (reportedly resulting in the need to reestablish access for all users), system access weaknesses were not included as a report finding.

Overall Risk Evaluation

High	Medium	Low
Inadequate management of City network accounts assigned to vendors and volunteers		
Use of generic network accounts		
	Inadequate control for ActiveNet system access	

Detailed Audit Findings

1. City network accounts, assigned to vendors and volunteers, were inadequately managed.

We reviewed 531 active CFW network accounts assigned to City vendors and volunteers, as of July 2019. Based on our review, 233 of those 531 accounts (44%) had not been used since the accounts were created. The retention of user accounts that are no longer needed creates the potential for inappropriate access of the CFW's network.

CFW Network Accounts by Department – Vendor and Volunteer Accounts

Department	Accounts Never Accessed			Total
	Vendor	Volunteer	Other	
City Manager's Office	5	1	0	**6**
Code Compliance	1	1	0	**2**
Fire	127	0	0	**127**
Information Technology Solutions	13	0	0	**13**
Municipal Court	4	2	0	**6**
Park and Recreation	2	0	0	**2**
Planning and Development*	19	0	0	**19**
Police	17	1	0	**18**
Transportation and Public Works	21	0	0	**21**
Public Health**	14	0	0	**14**
Unknown	4	0	1	**5**
Total	**227**	**5**	**1**	**233**

Source: Information Technology Solutions Department

* Department name changed to the Development Services Department, effective January 4, 2020

** Department discontinued in FY2009

Although the accounts had not been used since they were created, five of the accounts appeared on the Information Technology Solutions Department's 2019 Security Training results summary as having taken the security training course.

The following table shows the calendar years in which the 233 unused CFW vendor and volunteer accounts were created, by department.

CFW Network – Vendor and Volunteer Accounts Never Accessed – Number of Accounts by Department

Calendar Year Account Created	City Manager's Office		Code Compliance		Fire	IT Solutions	Municipal Court		Park & Recreation	Planning & Development*	Police		TPW	Public Health**	Unknown		Total # Accounts
	Vendor	Vol	Vendor	Vol	Vendor	Vendor	Vendor	Vol	Vendor	Vendor	Vendor	Vol	Vendor	Vendor	Vendor	Other	
2001	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	**1**
2003	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	**1**
2008	0	0	0	0	0	1	1	0	0	0	1	0	2	0	0	0	**5**
2009	2	0	0	0	8	0	0	0	0	0	3	0	0	14	0	0	**27**
2010	3	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	**5**
2011	0	0	0	0	117	0	0	0	0	0	1	0	0	0	0	0	**118**
2012	0	0	0	0	0	0	3	0	0	0	4	0	1	0	0	0	**8**
2013	0	0	0	0	0	0	0	0	0	7	2	0	1	0	0	0	**10**
2014	0	0	0	0	1	0	0	0	0	2	0	0	2	0	0	0	**5**
2015	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	**2**
2016	0	0	0	0	0	0	0	0	1	1	0	0	1	0	4	0	**7**
2017	0	0	0	0	1	5	0	0	0	1	1	0	2	0	0	0	**10**
2018	0	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	**3**
2019	0	1	1	1	0	4	0	2	0	6	3	0	10	0	0	0	**28**
Unknown	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	**3**
Total	**5**	**1**	**1**	**1**	**127**	**13**	**4**	**2**	**2**	**19**	**17**	**1**	**21**	**14**	**4**	**1**	**233**

Source: Information Technology Solutions Department

* Department name changed to the Development Services Department, effective January 4, 2020
** Department discontinued in FY2009

Approximately 50% of the accounts, which had not been used since being created, were vendor accounts assigned to the Fire Department in 2011. Based on our analysis, these accounts appear to have been created for an emergency operations center exercise. For example, some accounts were assigned to individuals representing the American Red Cross, Tarrant County, etc.

The Control Objectives for Information and Related Technology (COBIT) standard states that user access rights should be maintained in accordance with business requirements and that all users, along with their activity on IT systems (business application, IT infrastructure and system operations) are uniquely identifiable. The COBIT standard also states that policies and procedures for the management of contract staff should be documented and implemented. The documentation should include formal agreements from contractors stating that they are required to comply with the enterprise's IT control framework, such as policies for security clearance, physical and logical access control, use of facilities, information confidentiality requirements, and nondisclosure agreements.

Network access agreements require that annually, vendors provide a list of personnel requiring access. A Vendor/Contractor VPN Access Request Form is used to list the personnel who require access. Section 11.5.3.4 of the City's Administrative Regulation D5, *Information Technology Security*, requires that volunteers sign a volunteer access acknowledgement. We could not locate forms for 28 of the 57 vendor and volunteer accounts tested. Copies of some forms were stored as attachments to ITS Help Desk tickets. However, separate copies of the forms were not retained.

Recommendation 1: *The Chief Technology Officer should require that policies and procedures are created and enforced to ensure that City network accounts are:*

- *disabled and removed from the City's network if the accounts are unused for a certain length of time and/or considered unnecessary (e.g., the vendor's contract has expired); and,*
- *periodically reviewed for usage and necessity.*

Auditee's Response: Concur.

Responsibility: Steve Streiffert, Assistant IT Solutions Department Director

Target Implementation Date: December 31, 2020

Applicable Department Head: Roger Wright, Interim Chief Technology Officer

Applicable Interim Assistant City Manager: Kevin Gunn

2. Generic CFW network accounts were used to access the City's network.

Three generic network accounts were used during the audit period to access the CFW's network in July 2019. The configuration of these generic accounts allows account use by multiple users. According to the Police Department (to which the accounts belong), the accounts' configurations only allowed access to City email and specific computer files.

Generic accounts and their use do not provide uniqueness, making it difficult to know who accessed a particular IT business application or network. The COBIT standard states that all users and their activity on IT systems (business application, IT infrastructure, and system operations) are to be uniquely identifiable.

Recommendation 2: *The Chief Technology Officer should ensure that generic accounts are deactivated and that individuals with assigned generic accounts are reassigned their own unique user account.*

Auditee's Response: Partially Concur. Since there are some generic accounts that are required (such as system administrative accounts), we cannot concur fully with this recommendation. Policy and processes are being established so that unique administrative accounts are being created for individuals to use instead of using generic accounts where possible. Where required, generic accounts use and access will be controlled and monitored.

Responsibility: Steve Streiffert, Assistant IT Solutions Department Director

Target Implementation Date: October 1, 2020

Applicable Department Head: Roger Wright, Interim Chief Technology Officer

Applicable Interim Assistant City Manager: Kevin Gunn

Audit Comment: The generic accounts identified during our audit were not related to system administrative accounts. Instead, they were related to specific network accounts. Internal Audit, therefore, strongly recommends that the generic accounts identified during this audit (and used to access the City's network) be deactivated. We do, however, agree that generic accounts are sometimes

required (e.g., when there are interfaces between systems where an account username and password are required). However, in instances where generic accounts are required, the use of and access to such accounts should be controlled and monitored, with appropriate system rights assigned to each account. The City's use of generic accounts was also mentioned in the FY2016 external audit.

3. Access to the City of Fort Worth ActiveNet system was not adequately controlled.

Internal Audit reviewed ActiveNet user accounts, and compared those accounts to a complete list of CFW network users. Our review showed that 65 ActiveNet user accounts were still active for individuals no longer employed with the CFW. It should be noted that during the audit, the Park and Recreation Department deleted the 65 accounts that were assigned to former City employees.

In addition, 95 accounts were identified as belonging to ActiveNetwork LLC employees, 29 of which had the ability to perform financial accounting-related functions, including the ability to modify ActiveNet general ledger accounts, customer account payment plans and balances, and journal entries that would be sent to the CFW's financial system for processing. We did not perform additional research to determine whether any of the ActiveNet employee users made inappropriate system changes, as this was considered outside the scope of the audit.

ActiveNet is software that provides citizens the ability to reserve and rent CFW-owned facilities such as parks, community centers, libraries, the Nature Center, and the Botanic Garden. It also provides CFW staff (across eight departments) the ability to manage those reservations. ActiveNetwork LLC, a company specializing in software for sports camps, collegiate sports teams, YMCAs, and local municipality parks and recreation operations, externally hosts the ActiveNet system.

Since ActiveNet system administrator personnel did not receive formal employee termination notifications from the PeopleSoft ERP Human Resources system, user accounts were not disabled as necessary. Without such notification, the ActiveNet system administrator would not necessarily know there are terminated employee ActiveNet accounts that need deactivation. As noted in the following table, terminated users with access rights have been identified in previous audits issued by the Department of Internal Audit.

Previously Released Internal Audits with Terminated Employee Access Findings

Audit Report	Issue Date
Procurement Card Program Audit	12/11/15
Planning and Development Software Audit	02/03/17
Procurement Process Audit	06/23/17
Fleet Maintenance Audit	10/20/17
ERP II Post System Implementation Audit	01/05/18
Hyperion Software Implementation Audit	03/29/19

Prior external audits have also identified control weaknesses related to the City's lack of formal procedures to review the appropriateness of system access (FY2017, FY2018 and FY2019).

The COBIT standard states that user access rights should be maintained in accordance with business requirements, accounts should be reduced to the minimum number necessary, privileged user accounts should be actively managed, and activity on all accounts should be monitored.

Recommendation 3A: *The City Manager should require that the Human Resources Director send the listing of terminated employees to department heads and direct the distribution to employees with system administration responsibilities.*

Auditee's Response: Concur. HRIS currently has available and distributes an Employee Term Report to departments that require it. By March 1, 2020, the departments that need it for ActiveNet can be added to the distribution list. Additionally HR will facilitate a review of the process to include adding position changes and potentially enhancing the report for departments by June 1, 2020.

Responsibility: Human Resources Department

Target Implementation Date: June 1, 2020

Applicable Department Heads: Brian Dickerson, Human Resources Director

Applicable Deputy City Manager: Jay Chapa

Recommendation 3B: *The Park and Recreation Director, in conjunction with the Chief Technology Officer, should ensure the number of ActiveNet vendor user accounts are periodically reviewed and access reduced to the minimum required.*

Auditee's Response: Concur.

Responsibility: [The] Park & Recreation ActiveNet Administrator receives a weekly report of terminated Park & Recreation, Neighborhood Services, Library and Fire Department employees and removes employee access from ActiveNet upon receipt. [The] ActiveNet Technical Account Manager also sends the PARD Administrator a list of users who have not accessed Active Net in the last 90 days and that access is removed as well. Security levels have been corrected to limit those who have financial or system management security.

Target Implementation Date: Completed

Applicable Department Heads: Richard Zavala, Park and Recreation Director

Applicable Assistant City Manager: Fernando Costa

Acknowledgements

The Department of Internal Audit would like to thank all City departments for their cooperation and assistance provided during this audit.