CITY OF
TORRANCE

DATE: 6/6/23

TO: Li Chang, Systems Analyst
Earl Kay, Systems Analyst
Stephen Lavey, Systems Analyst
Michael Pan, Systems Analyst

FROM: Jason Nishiyama, Deputy Finance Director

SUBJECT: Information Technology General Controls Review - User Access

Enclosed is the final audit report for the Information Technology (IT) General Controls Review - User Access. Internal Audit would like to thank you and your staff for the support and assistance provided to us during the audit.

Should you have any questions, please feel free to contact Fulton Bell (Senior Auditor) or Debbie Quach (Auditor).

Thank you,

Enclosure

Cc: Aram Chaparyan, City Manager
Danny Santana, Assistant City Manager
Jay Hart, Police Chief
Sheila Poisson, Finance Director
Michelle Ramirez, Community Development Director
Patrick Sullivan, City Attorney
Andrei Yermakov, IT Director

CITY OF TORRANCE

INTERNAL AUDIT SERVICES

Information Technology (IT) General Controls Review User Access

May 19, 2023

Table of Contents

Audit Overview 1

- Background 1
- Audit Objective 1
- Scope & Approach 1

Executive Summary 2

Summary of Findings 3

Audit Overview

Background

Windows accounts and user accounts for applications are created by Communications Information Technology (CIT) Systems Analyst for employees at the request of Department management. Access to City's systems should only be granted, maintained and accessed by authorized users with justified use for their jobs. All user accounts should be reviewed periodically by management to ensure compliance with the City's technology and information security policies.

Audit Objective

The objective of the audit was to verify user access to Windows Active Directory (AD), Accela, New World and ADP by identifying terminated and inactive users, shared accounts, and accounts with no activity greater than 12 months.

Scope

The scope of the audit included accounts from the following systems: Windows AD, ADP, Accela, and New World. The data used for testing contained information as of December 2022 and January 2023. In addition, we requested from Payroll division hiring packets for testing.

Approach

To achieve the audit objectives, the following procedures were performed:
- Requested from CIT Systems Analyst the employee list from ADP for December 2022. The information is extracted daily from ADP via their reporting system and imported into a local database daily. The report contains information such as employee ID, name, payroll unit, network account, email address, date of hire, and employee title.
- Requested from CIT Systems Analyst the New World users list. The report contains information such as log in ID, user name, log in IP address, days since last log in, and last log in date/time.
- Requested from CIT Systems Analyst the Accela users list. The report contains information such as user ID, module, security group, department, last login date, and email address.
- Requested from CIT Systems Analysts the Windows AD list for City Hall employees and Torrance Police Department (TPD).
- Requested from TPD volunteer program coordinator a list of volunteers in the Police Department.
- Tested the accuracy of the employee list from ADP by selecting a sample of 15 new hires from October-December 2022 and verified the information on the list with the hiring packet in Payroll. The fields compared were employee ID, name, payroll unit, hire date, and grade.
- The ADP employee list was used to compare New World users by log in ID, Accela users by email address and Windows AD by account name. The comparisons were done by using the VLOOKUP function in Excel.

Executive Summary

We identified issues for improvement which are summarized by risk rating to the right. The identified issues were discussed with appropriate staff and remediation has started regarding the following:

- Terminated employees, inactive volunteers, and unauthorized users had active Windows accounts. Management should immediately deactivate accounts that are no longer required.
- System accounts that were unused for several years, did not have justification for remaining active. Unused user accounts should be assessed regularly and accounts disabled as appropriate.
- Generic and shared user accounts that were not tracked and assigned.

Access to key systems should be strictly controlled at all times to help ensure security and confidentiality of information system resources.

All findings were reviewed with appropriate staff and a Citywide Information Security Policies were implemented to assist with enforcement and compliance.

Priority 1
Critical control weakness that exposes the City to a high degree of combined risks.
Windows Active Directory (AD) user accounts should be reviewed regularly to help ensure only authorized users have access to City information system resources.
Priority 2
Less than critical control weakness that exposes the City to a moderate degree of combined risks.
Use of generic and shared user accounts should be minimized because activity is difficult to track and accountability assessed.
Priority 3
Opportunity for good or better practice for improved efficiency or reduce exposure to combined risks.
n/a

Summary of Findings

Windows Active Directory (AD) user accounts should be reviewed regularly to help ensure only authorized users have access to City information system resources.

		Finding	Recommendation	Auditee Response & Action Plan Due Date
Priority 1	1	**Torrance Police Windows Accounts** We found 84Torrance Police Department (TPD) Windows AD accounts that should be reviewed by Systems Analyst to determine if any of the accounts can be disabled. Of the 84 accounts, 7 were individual accounts that were not current employees or volunteers and 77 were shared/generic accounts.	We recommend TPD Systems Analyst to create individual user accounts instead of shared accounts whenever possible. If a shared account must be kept, controls are to be implemented to ensure the accounts are being monitored by IT. Unused accounts should be disabled immediately. TPD volunteer program coordinator should notify IT when a volunteer is inactive.	We spoke with TPD Systems Analyst and the following actions were agreed upon: - 33 accounts will be disabled because they are either shared accounts, unused accounts, or the volunteer/employee is no longer employed by the City - 9 accounts will be investigated further by TPD Analyst before potentially disabling - 2 accounts will temporarily be kept waiting for Office of Emergency Services (OES) to research further - 1 shared account will be kept because disabling it would affect IT staff. Monitoring controls will be implemented by TPD IT - 1 shared account used among the volunteers in Records will temporarily be kept until IT can create individual accounts - 3 test accounts will be disabled and enabled as needed instead of keeping them active all the time - Target completion date: June 30, 2023.
	2	**City Hall Windows Accounts** We found 485 City Hall Windows AD accounts that should be reviewed by Systems Analyst for possible disabling. Of the 485 accounts, 14 were individual accounts that were not current employees and 471 generic/shared accounts.	We recommend Windows Systems Analyst to review the 14 individual accounts and 471 shared/generic accounts and verify if any can be disabled. Systems Analyst should work with the departments to disable shared accounts and create individual accounts when possible and continue to disable unused accounts at the departments request.	Eleven employee accounts and 151 generic accounts that Systems Analyst identified were no longer needed were disabled. On 4/27/23, seven additional accounts were disabled at the request of Community Services Department. Systems Analyst will continue to disable unused accounts at the departments request. - Target completion date: June 30, 2023.

Summary of Findings

Use of generic and shared user accounts should be minimized because activity is difficult to track and accountability assessed.

		Finding	Recommendation	Auditee Response & Action Plan Due Date
Priority 2	1	**New World Accounts -Generic Accounts** Based on review of the New World account listing we found 3 active accounts that were shared/generic accounts. Shared and generic accounts should be minimized to help ensure tracking and accountability of system activities.	We recommended Systems Analyst review the 3 shared/generic accounts to determine if they can be disabled. Account tempuser is a guest account and should be enabled/disabled as needed. It should not be kept active all the time.	Systems Analyst will enable/disable account tempuser as needed. The account was disabled on 4/13/23. In addition, one employee and one generic account were also disabled. - Target completion date: April 13, 2023.
	2	**New World Accounts - Inactive Users** There were 22 New World accounts that had not logged into the system for a year or more.	We recommended all 22 accounts be disabled due to non-activity. At the request of the departments, 19 accounts will be kept active and disable 3 accounts. For the accounts the departments decided to keep, although there are no activity, controls should be implemented to monitor those accounts.	System Analyst will disable 3 accounts the departments determine were no longer needed. The 3 accounts were disabled on 4/13/23. - Target completion date: April 13, 2023.
	3	**Accela Accounts** Based on review of the Accela account listing we found 78 active accounts that were shared/generic accounts. Shared and generic accounts should be minimized to help ensure tracking and accountability of system activities.	We recommended 23 shared accounts be deactivated and individual accounts be created. Disable 26 accounts that the departments no longer needed.	We spoke with CIT Systems Analyst and the following actions were agreed upon: - Systems Analyst will disable 23 shared accounts and create individual logins. - Disable 26 accounts that the departments no longer needed As of 4/3/23, five shared accounts have been disabled and individual accounts created. In addition, twenty-six unused accounts have been disabled. Will follow-up with System Analyst regarding the other shared accounts. - Target completion date: March 17, 2023.