INTERNAL AUDIT REPORT

2023-03

Infor Public Sector Access Controls

Information Technology Department

June 23, 2023

MUNICIPALITY OF ANCHORAGE
Office of Internal Audit
632 W 6th Avenue, Suite 710
P.O. Box 196650
Anchorage, Alaska 99519-6650
www.muni.org/departments/internal_audit

OFFICE OF INTERNAL AUDIT
Michael Chadwick, CIA, CICA
Director
Phone: (907) 343-4438

E-Mail: michael.chadwick@anchorageak.gov

MUNICIPALITY OF ANCHORAGE
MAYOR DAVE BRONSON

OFFICE OF INTERNAL AUDIT

June 23, 2023

Honorable Mayor and Members of the Assembly:

I am pleased to present for your review **Internal Audit Report 2023-23, Infor Public Sector Access Controls, Information Technology Department**. A summary of the report is presented below.

In accordance with the 2023 Audit Plan, we have completed an audit of the Infor Public Sector software system. The objective of this audit was to determine whether access controls to the Infor Public Sector Software system for Municipal employees and supporting staff were adequate and complied with applicable policies and procedures. Our audit included a review of the Infor Public Sector Software system user account records maintained by the Information Technology Department. Specifically, we compared active user account records to current Municipal employee and contractor records.

We found access controls to the Infor Public Sector Software system for Municipal employees and supporting staff can be improved. Specifically, we found that the Infor Public Sector Software system user accounts for terminated employees were not always deactivated in a timely manner. Moreover, the Municipality of Anchorage did not possess the Infor Public Sector Software system licensing agreement and the Infor Public Sector Software system user account password requirements and controls were not activated.

There were three findings in connection with this audit. Management was responsive to the findings and recommendations in this report.

Michael Chadwick, CIA, CICA
Director, Internal Audit

MUNICIPALITY OF ANCHORAGE
MAYOR DAVE BRONSON

OFFICE OF INTERNAL AUDIT

June 23, 2023

Internal Audit Report 2023-03
Infor Public Sector Access Controls
Information Technology Department

Introduction. The Municipality of Anchorage (Municipality) uses the Infor Public Sector (Infor) software system to streamline community development and regulation functions. Infor supports processes such as electronic management and automation of business applications, permitting, geographic information systems land management, and service requests.

Access to Infor is managed by the Information Technology Department (IT) who establishes new accounts and usernames only in response to valid supervisor requests based on business needs, usually for new employees during the onboarding process. Similarly, once access is no longer required to support business needs, usually due to employee transfer or termination, notice is sent to IT to deactivate system access for that user's account.

Objective and Scope. The objective of this audit was to determine whether access controls to Infor for Municipal employees and supporting staff were adequate and complied with applicable policies and procedures. Our audit included a review of Infor user account records maintained by IT. Specifically, we compared active user account records to current Municipal employee and contractor records.

We conducted this performance audit in accordance with generally accepted government auditing standards, except for the requirement of an external quality control review. 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. The audit was requested by the Administration.

Overall Evaluation. Access controls to Infor for Municipal employees and supporting staff can be improved. Specifically, we found that Infor user accounts for terminated employees were not always deactivated in a timely manner. Moreover, the Municipality did not possess the Infor licensing agreement and Infor user account password requirements and controls were not activated.

FINDINGS AND RECOMMENDATIONS

1. Infor User Accounts for Terminated Employees Not Always Deactivated.

a. **Finding.** Infor user accounts for some terminated employees were not always deactivated. Specifically, 12 user accounts were still open after the employees had been terminated. According to IT staff, four of these accounts belonged to senior managers and were being held open at the request of the Development Services Department to preserve saved user data and queries. At the time of this audit, these accounts had been open from 304 days to 419 days. To safeguard these accounts, IT changed the passwords to prevent access by unauthorized personnel. The remaining eight user accounts belonged to former Municipal employees and were still active 3 to 87 days after the employees' last day worked, according to Human Resources records. As these accounts still had valid usernames and passwords, it was technically still possible for the terminated employees to access these accounts without any valid Municipal business purpose. Although Development Services staff notified IT regarding the terminations for their employees, IT staff could not explain why these accounts had not been deactivated. Active user accounts for terminated employees present a security risk to the Municipality's information systems.

Policy and Procedure (P&P) 28-9, *Business Use and Access Control*, states that "Personnel must use MOA networks and associated systems for authorized purposes only, related to MOA business and their job duties . . ." and "Personnel must not access MOA information, programs, or systems when such access is not required for an authorized business purpose." In addition, the National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organization*s, directs that when an individual terminates employment the employer should disable access to the system and "Terminate or revoke any authenticators and credentials associated with the individual."

b. **Recommendation.** The IT Director should ensure that Infor user accounts for terminated Municipal employees are deactivated promptly.

c. **Management Comments.** Management stated, "The IT Management concurs with the finding and recommendation. The following actions have or are being taken to correct the situation:

- Deactivate all Infor accounts for terminated employees.
- Establish a written process to review user accounts quarterly.
- Activate a process to save and transfer data and queries from terminated employees to current employees.
- Collaborate with Development Services to write a Memorandum of Understanding establishing roles and responsibilities.
- Create/refresh training material and documentation.
- Integrate Infor with Active Directory services."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

2. Infor License Agreement Not Available.

a. **Finding.** The Municipality did not possess the Infor licensing agreement. No one at the Municipality, including IT staff, could provide us a copy of the Infor license agreement or data to support the licensing agreement. As a result, without maintaining a copy of the Infor license agreement and data to support the agreement, the Municipality had no way of determining whether it complied with the agreement, or whether it may be subject to penalties for non-compliance. For example, without the licensing agreement we could not determine if the Municipality was using more licenses than permitted by the agreement.

An Infor license agreement we found online states that the "By installing the software you indicate that unless there is a separate manually signed license agreement between Licensee and Infor, on behalf of the Licensee, you accept the terms and conditions of this Agreement as governing the license of software to Licensee." Further, on Infor's website the frequently asked questions section states that, "Infor periodically reviews its license agreements with customers to ensure compliance." In addition, "Infor recommends the following tips to ensure you remain in compliance with your signed license agreement.

- Understand license agreement terms in detail.
- Maintain accurate application and database usage records.
- Maintain accurate hardware environment records."

b. **Recommendations.** The IT Director should ensure that all Infor user license agreement(s) and supporting data are readily available, and that all terms and conditions stated within the agreement are always met.

c. **Management Comments.** Management stated, "The IT Management concurs with the finding and recommendation. The following actions have or are being taken to correct the situation:

- IT requested and received all current and executed license agreements from Infor.
- Collaborate with Development Services to write a Memorandum of Understanding establishing roles and responsibilities.
- Perform annual review to ensure compliance with the terms of our license agreements."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendations.

3. Infor User Account Passwords Not Actively Managed.

a. **Finding.** Infor user account password requirements and controls were not activated. Specifically, the Infor administrator password settings control panel did not specify any required user password parameters or settings. These settings included minimum requirements for the use of mixed case, numeric, and special characters, minimum password length, password history, maximum days until expiration, and allowed number of login attempts. According to IT staff, they did not know why there was nothing configured or enabled in the administrator password settings section.

Policy and Procedure 28-7, *Password Management*, requires that "Personnel must set a password of sufficient length and complexity according to the following standards: ...The password length must be 14 characters or more...must contain a combination of upper and lower case letters and include at least one numeric and/or special character. . ." and "...shall not be any of your previous 10 passwords."

Additionally, P&P 28-7 also requires IT staff to "Ensure that password history is enabled...", that "...password expiration does not exceed 365 days...", and finally to "Review users' access rights to systems at a minimum of once a quarter." Failure to enforce the required password controls established by P&P 28-7 may present a security risk to the Municipality's information systems.

b. **Recommendation.** The IT Director should ensure that all Infor user password controls are properly enabled and enforced as required by P&P 28-7.

c. **Management Comments.** Management stated, "The IT Management concurs with the finding and recommendation. The following actions have or are being taken to correct the situation:

- Enable password controls consistent with P&P 28-7, to the extent it is supported.
- Collaborate with Development Services to write a Memorandum of Understanding establishing roles and responsibilities.
- Document manual process to maintain compliance with P&P 28-7 while using Infor and share with department heads."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

Discussion With Responsible Officials. The results of this audit were discussed with appropriate Municipal officials on May 22, 2023.

Audit Staff:
Derek Reynolds