USER ADMINISTRATION

PROGRAM EVALUATION AND AUDIT

METROPOLITAN COUNCIL

Contents

Highlights

Employee Termination and User Administration Procedures Need Improvement

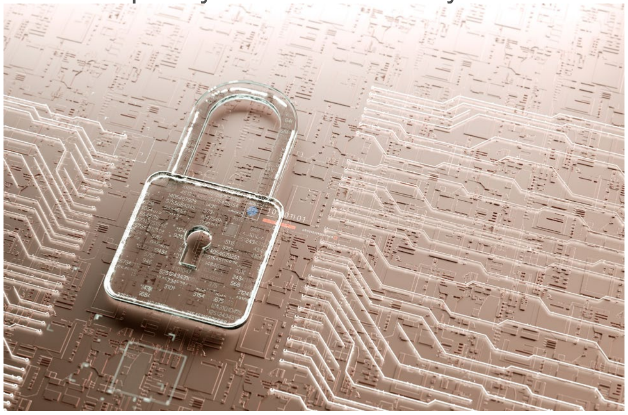
What We Found

What's Working Well

IS implemented an automated process for disabling network accounts for some portions of the Council's network in March 2022. HR has implemented some processes to increase accountability for late employee terminations in response to the OSA findings.

What Needs Improvement

Policies and procedures for user administration should be periodically updated to include industry best practices. Specifically, the *Separation of Employment Procedure* does not include guidance for all steps of the termination process. Managers are not regularly trained on how to execute employee terminations and use of the *Leaving Service Form*. Currently there are many steps in the termination process involving multiple departments, which adds complexity and leads to delays.



What We Recommend

An Identity and Access Management (IAM) Program should be developed. Policies, procedures, trainings, and work instructions should be revised to support the IAM program with Center for Internet Studies (CIS) and National Institute of Standards and Technology (NIST) best practices. The Regional Administrator and Senior Management should commission and hold staff accountable for implementing the IAM, including implementation of Role Based Access Controls for managing user accounts within HR and IS procedure.

Why We Did This Work

Given the history of Office of State Auditor (OSA) findings related to late employee terminations and the risk of late terminations, Audit initiated an audit to review employee records management and the processes related to user administration to better understand the state identity and access management at the Council.

What We Reviewed

Audit conducted interviews, reviewed HR and IS policies and procedures, as well data related to user administration activities from 2020 and 2021. Audit focused on user role creation, role assignment, periodic access reviews, and user terminations.

How We Did This Work

Audit completed tests on PeopleSoft user roles, periodic access reviews, and employee termination data and summarized observations. Audit reviewed IS data relating to network access termination and summarized observations. Managers, HR staff, and IS staff were interviewed about the process they follow to terminate employee and manage system access.

Summary of Findings

Number	Description	Recommendation	Follow-up Action	Page
Observation 1	Policies and procedures for user administration are not informed by industry standards or best practices.	Identity and Access Management program and approving associated technology standards. In the interim, IS and HR should define and apply the required security standards for high-risk accounts that may require immediate termination due to involuntary employee terminations.	Assess Risk	9
Observation 2	The Council has not implemented Role Based Access Controls (RBAC).	The Council should establish RBAC for the PeopleSoft Financials, PeopleSoft HRMS, Active Directory and Office 365 system per NIST or (CIS) best practices.	Assess Risk	11
Observation 3	A large number of late employee terminations, complicating the Council's user identity management.	HR staff should minimize late terminations and document the reason for late terminations.	Retest	12
Observation 4	Managers and IS Staff have not consistently terminated network user accounts in a timely fashion.	IS should establish a risk-based timeliness metric and terminate network access in a timely fashion for terminated employees.	Assess Risk	14

Introduction

Background

Identity Management – also known as Identity and Access Management, (IAM)—"is the set of procedures to issue and manage digital identities of people and systems so that they can be uniquely authenticated to IT systems before being granted online access to sensitive IT assets. Such assets include computer systems, digital information in structured or unstructured formats, databases, web and database servers, email and video systems, and assets with report generation capabilities”[1]. User administration is a component of IAM, and should include procedures for hiring, transferring, and terminating employees, issuing system account access, periodically reviewing access, and terminating user access.

Role Based Access Controls (RBAC) is an approach to restricting system access to authorized users. RBAC includes creating roles based on a user’s business need and restricting access to provide the least privilege necessary for the position. Roles should then be assigned to individuals based on their position at the organization. According to the National Institute of Standards and Technology (NIST), policy and procedure should be used to assign managers or directors as data owners and given responsibility for the integrity, accurate reporting, and granting the use of data accessed by users. Periodic access reviews by data owners should be conducted to confirm the access assigned to a role is appropriate for a given position, and that the individuals assigned access roles should still be granted access to that role. System owners should also be defined, and support data owners in provisioning, reviewing, and terminating user access.

The Council’s Technology Governance Policy states that, “As the Accountable Authority, the Regional Administrator will appoint the Chair of the Enterprise Service Planning Team (ESPT). The ESPT consists of division level senior executives. The Regional Administrator will work with the ESPT to define and approve the roles and responsibilities for the individuals and groups involved with technology governance at the Council.” This establishes the Regional Administrator as being accountable for “commissioning and approving” technology security standards, such as those security standards that would implement an identity and access management program and RBAC. Currently the Council’s policy is to disable accounts when employees have separated from the Council. The Council currently has two procedures for employee termination, the HR Separation of Employment of Procedure – HR 7-1 and the IS Inactive User and Vendor Account Management procedure – Tech 2-1h. The HR procedure addresses the different forms of separation of employment and information about actions to be taken for each type of separation. The IS procedure addresses terminating user network accounts and associated credentials for terminated employees, and the timeframe within in which to complete procedures. The manager is responsible for filling out a Leaving Service Form to notify HR of the individual’s end of employment. If the Leaving Service Form is not completed, there is a IS backup process mandated by procedure in which IS staff terminate user account access. The IS procedure states that accounts should be disabled after 30 days of inactivity and deleted 30 days after the account is disabled.

[1] Identity Management Audit/Assurance Program [ISACA], 2013. P. 11

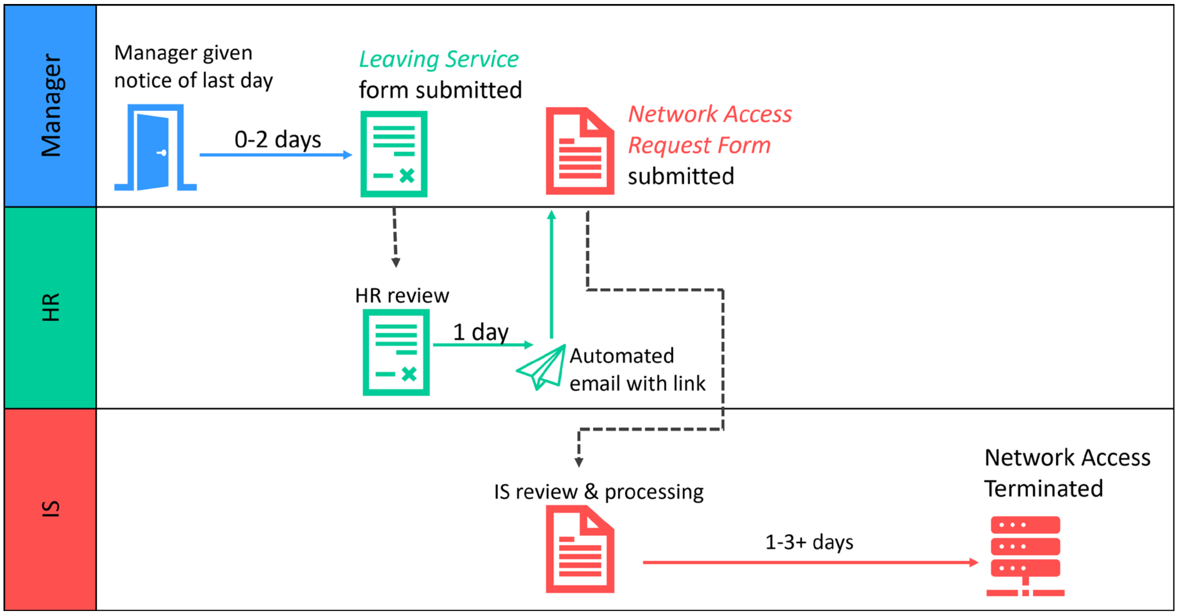

Manager
HR
IS
Manager given notice of last day
0-2 days
Leaving Service form submitted
Network Access Request Form submitted
HR review
1 day
Automated email with link
IS review & processing
1-3+ days
Network Access Terminated

Figure One: Diagram of termination processes, noting responsibilities by process actor

Over the last couple of years, the Office of the State Auditor (OSA) has issued written findings regarding the late termination of employees and untimely revocation of access for terminated employees. When employees leave employment with the Metropolitan Council, their access to all computer systems, networks, and data should be removed within 14 days per the OSA. Per the OSA audits, there were no audit trails, and HR and IT were not able to provide the date of the removal of employee access.

Following the 2019 OSA Audit, a corrective action plan was implemented regarding the *Separation of Employees procedure*, to increase accountability terminating employees and user account disablement by September 30, 2020. Following the 2020 OSA Audit, a second corrective action plan was implemented to increase the auditing of the *Leaving Service Form* for compliance with HR policy and improve IS Staff's account disablement by August 31, 2021.

Objective

The purpose of this audit is to evaluate the controls which the Council has developed and implemented for user administration. The audit evaluated the policies, procedures, and tools for ensuring users have appropriate access to technology resources, and the extent to which practices minimize business and technology security risks. The audit additionally reviewed the extent to which Council policies and procedures implement best practices described in the NIST Critical Infrastructure (CI) Framework, and Center for Internet Studies (CIS) guidance related to identity and access management. Additionally, we considered the implementation of user administration related procedures and processes by HR staff for employee terminations, to review corrective actions related to findings by external auditors. Lastly, we reviewed the implementation of procedures and processes by IS staff related to terminating employee network and email access, to review corrective actions related to findings by external auditors. Internal Audit considered the Council's *Thrive MSP 2040* outcomes of Stewardship.

Scope

The scope for this audit included all available user administration documents, policies, procedures, and tools. The audit scope included the activities pertinent to user administration such as establishment (provisioning), termination (revocation), access reviews, and maintenance of user identities within PeopleSoft Financials, PeopleSoft HRMS, Microsoft Active Directory, and Office 365. The audit examined user administration activities from January 2020 through December 2021.

Methodology

Audit conducted interviews with various managers and staff in HR and IS departments to review the processes behind access management, and employee hires, transfers, and terminations and the obstacles that may prevent the timely completion of these processes. We compiled user termination data from 2020 to 2021 to analyze the frequency of late terminations and to analyze the extent to which the causes of late terminations could be documented. We completed walkthroughs with IS and HR staff who perform of termination processes. We tested HR and IS termination data from 2020-2021, as well as a sample of 20 terminations stratified by Division, reason for termination, and the number of days late the termination was processed, to evaluate how well the actual terminations processed complied with HR and IS policies and procedures.

Internal Audit reviewed employee terminations across the Metropolitan Council between the Jan. 1, 2020 – Dec.18, 2021. We analyzed HR processes for terminating employee, including the frequency and reason for late terminations. Audit established lateness by using the employees last day worked as entered in HRMS as the termination “Effective date” field in the HRMS system. When HR completes an action in HRMS, the system logs the date in the “action entered” field. Audit compared the “effective date” to the “action entered date” to determine how long it took for HR to process the termination. Audit then considered the employee termination date next to access changes related to IS network access.

Limitations

Internal Audit noted significant barriers to analyzing user administration activities due to a lack of activity documentation in the form of policies, procedures, work instructions, or job aids. Additionally, Internal Audit noted a lack of documentation to justify late employee terminations, and the lack of documentation to answer questions related to why terminations were processed late. Network activity and log data and retention schedules were limited, as systems used to add or remove access were not configured to retain data necessary to log activity and support audits of user administration.

Recognition

Program Evaluation and Audit appreciates the assistance HR and IS departments provided during the audit. We are encouraged by the response to the issues identified and recommendations made within this report, Council staff were forthcoming and helpful during interviews, written responses, document reviews, and in obtaining source data and materials.

Observations

Council policies and procedures for identity and credential management are not informed by industry standards or best practices.

Human Resources (HR) and Information Services (IS) procedures are not linked to an Identity and Access Management Program (IAM). HR and IS Staff have not defined roles and responsibilities for identity and credential management within procedures that is informed by industry standards or best practices. Several HR and IS processes, policies, and procedures exist to manage user identities and credentials. The Council's current process involves coordination between Council Managers and Supervisors, the HR Department, and the IS department. Adding and terminating employee access at the Council involves two distinct processes, one for HR to add or terminate employees, and another for IS to add or terminate network and email (and Office 365 suite) account access.

The Council's *New Employee Orientation and Onboarding Procedure* (HR 7-1k) does not include guidance on access provisioning or a step to complete the *Network Access Form* for new employees to gain access to Council network drives. While IS has a process to grant access to new users, the use of the *Network Access Form* is not documented in IS policies, procedures, or work instructions. Neither the form nor procedure specifically address identity provisioning, identity reviews, or other aspects of identity management.

User administration Procedures and Forms	
HR Processes	IS Processes
• Includes: ○ *New Employee Orientation and Onboarding Procedure* ○ *HR Transfer Procedure* ○ *Separation of Employment Procedure*	• Includes: ○ *Inactive User and Vendor Account Management Procedure* ○ *Network Access Form*

See Appendix C for more information:

Specifically, neither the HR procedure, nor HR trainings provide guidance on what position Action or Reason option managers could use for the different types of employee new-hires, transfers, or terminations. While there are training videos regarding processing employment actions in the HRMS system, the trainings and procedure do not document specific guidance for HR and managers to assist them in determining and processing the appropriate reason code for a termination.

Management

- There are 475+ managers and supervisors Council-wide who do not receive specific or regular training on hiring, transferring, and terminating employees
- Mangers must submit separate forms to HR Staff and IS staff for every change in employment
- Managers may not understand proper use of HR and IS forms and codes

See Appendix B for more information

The Regional Administrator (RA) has not mediated a proactive tone at the top to create a cross-division, cross-functional IAM program. The RA did not create responsibility and accountability that ESPT development and approve technology security standards for user administration or Identity and Access management standards, as required by the Technology Governance Policy approved by the Council in 20180. As the tasks are carried out by multiple teams, there are multiple processes and timelines that depend on each other and create complexity and delays in processing terminations.

Without effective user administration procedures or technology standards, and controls may fail to manage employee termination in a timely fashion. When not following effective technology security standards for identity management, there is a greater risk that employees may have unauthorized access and damage Council systems.

Recommendation:

1. The Regional Administrator should hold the ESPT (or other designee(s)) accountable for commissioning an Identity and Access Management program and approving associated technology standards. Senior management should hold HR and IS accountable for ensuring their policies and procedures support the IAM program, based on NIST and CIS guidance. Policies, procedures, and trainings should ensure that employee access is terminated in a timely manner when an employee transfers to a new position or leaves employment with the Council and include a process for emergency terminations.

In the interim, IS and HR should define and apply the required security standards to be implemented for administrator accounts, privileged accounts, and other high-risk accounts that may require immediate termination due to involuntary employee terminations.

Management Response: Management agrees with the recommendation. The Regional Administrator will hold the ESPT (or other designee(s)) accountable to do so or appoint another group or leader to create an Identity and Access Management program and associated technology standards as part of building a wider comprehensive set of cyber security standards that align with industry best practices and applicable regulations.

Timetable: March 31, 2024

Staff Responsible: Mary Bogie (Regional Administrator), George Gonzalez (Deputy Regional Administrator)

Audit Follow-Up: Assess Risk

The Council has not implemented Role Based Access Controls (RBAC).

Processes for permission management and authorization are not documented in an established policy, procedure, or work instruction, according to technology security standards related to user administration. The Administrative Systems Support Services (AdSSS) department within Regional Administration Finance has been responsible for administering the PeopleSoft Finance and HRMS system, while Information Services (IS) administers Active Directory network access and access to the Office 365 suite of software. Both Admin Systems Support staff and IS Staff have created user roles with role names, but limited information is available on the access associated with roles.

Details regarding how Admin Systems Support staff and IS staff created system access roles, and the access assigned to the role, is not documented. There is limited information on how roles were defined for PeopleSoft and AD system access. Users can be assigned to different groups with assigned roles with specific permissions. For example, policy can be used to assign view only access for user of applications for a specific group of users (below, user Group-1) given a business need. Also, another user can be assigned a role that can view and edit application data in a section group (below, Group-2) which can be specified in a second policy. The edit access given to Group-2 applications are restricted for Group-1 as Group-1 is not granted authorization to edit application data per policy.

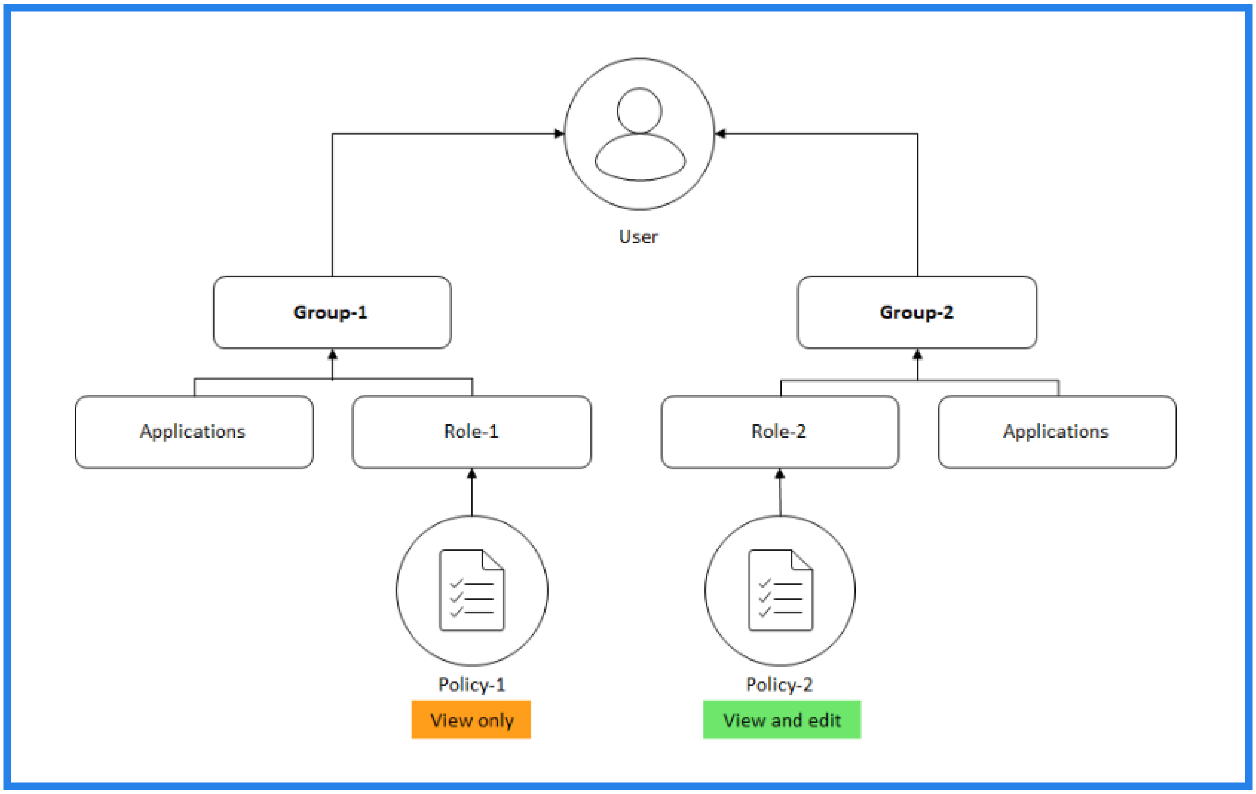


Figure Two: https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/access-control/role-based-access-control/rbac-configuring-groups.html#how-user-access-changes-based-on-the-authorization-scope.

While there are limited annual access reviews, neither AdSSS staff or IS staff have worked with data owners in conducting periodic access reviews for the PeopleSoft Financials, PeopleSoft HRMS, Active Directory (AD) network or O365 systems. No policies or procedures currently establish the roles and responsibilities for data owners and system administrators for access management. No procedures require that roles are created based on business need, incorporate the principles of least privilege and separation of duties, that roles are assigned to employees, and the access assigned to roles is reviewed on a periodic basis.

Neither the Regional Administrator nor the Enterprise Services Planning Team (ESPT) ensured that Council technology security standards were developed that mandated RBAC. Per the Tech Governance Policy:

The ESPT serves a leadership role in defining and directing all technology activities at a high level through review and approval of: (1) the Technology Strategic Plan; (2) technology principles, procedures, and standards; (3) the threshold and criteria that determine the selection procedure for given IT and OT projects; and (4) subgroup charters. Subgroups will provide technical expertise, feedback, cross-divisional awareness, and budgetary oversight that facilitates appropriate cost benefit analyses.

Without oversight, Admin Support Systems staff and IS staff failed to document how roles are established based on business need and position. Additionally, Senior Management did not support the definition of data and system owner roles and responsibilities. Without clear data and system owners being established, access reviews for the PeopleSoft Financial, HRMS, and Microsoft AD and O365 system were not formalized to incorporate NIST or CIS best practice. Without periodically reviewing the roles assigned to employees, the Council risks allowing access that may affect the confidentiality, integrity, or availability of Council systems and data. Without initial and periodic user role reviews by data and system owners, the Council risks assigning access to roles, and roles to individuals, which may exceed the access necessary to fulfill and employee's job.

Recommendation:

1. The Council should establish Role Based Access Controls for the PeopleSoft Financials, PeopleSoft HRMS, Active Directory and Office 365 system per National Institute of Standards and Technology (NIST) or Center for Internet Studies (CIS) best practices. RBAC should assign roles and responsibilities and define data and system owners for access administration. Data and system owners should have defined roles and responsibilities related to access management.

Management Response: Management agrees with the recommendation. The Council is undergoing a major Enterprise Resource Planning (ERP) project titled Business Processes Systems Integration (BPSI). The Council will implement role-based access control for the systems implemented as part of BPSI or significantly impacted by the BPSI project including PeopleSoft.

Timetable: The BPSI project is projected to be completed by 2026 including role RBAC elements. RBAC maybe completed earlier if an IAM program as outlined in recommendation 4 is approved.

Staff Responsible: Mary Bogie (Regional Administrator), George Gonzalez (Deputy Regional Administrator)

Audit Follow-Up: Assess Risk

Managers and HR staff processed a large number of late employee terminations, complicating the Council's user identity management.

In total, Manager and HR actions processed 143 of 964 employee record terminations more than 3 days after the termination effective date, making approximately 15% of all terminations late from January 1, 2020, to December 18, 2021. HR processed 44 terminations with "action entered" dates 14 days or more from the individual's departure date, approximately 4.55% of total terminations from January 1, 2020, to December 18, 2021. The number of late employee terminations resulted from flaws in the control environment regarding timely processing of employee terminations, and monitoring activities regarding the timeliness of HR processes.

Late Terminations by Division

Division	Late Terminations
Metro Transit	113 of 143 (73.02%)

Environmental Services	9 of 143 (6.29%)
Regional Administration (including Metropolitan Transportation Services and Community Development)	20 of 143 (13.99%)

HR processed one termination 353 days from the individual's departure date, due to the individual's manager not submitting the HR required paperwork to terminate the temporary employee. Additionally, this individual was paid a benefit over the course of the year, though the individual did not have a timecard submitted with hours worked during pay periods where they received the benefit. Though the payments made to the employee per pay period over this timeframe was not considered material, HR policy and the Payroll Department failed to ensure controls were implemented to confirm benefits are only paid when allowable.

A sample of 20 late terminations revealed timeliness and documentation issues by both managers and HR staff in the termination process. The reason for some late terminations could be established (for example, lateness related to HR staff processing entries late). However, 9 of 20 late employee terminations sampled did not have a documented reason for the late termination. For 8 of 20 terminations, we could not determine manager timeliness in submitting the *Leaving Service Form* (within 2 days of termination) because manager submission dates were not recorded. For 4 of the 20 terminations, managers did not understand how to use the *Leaving Service Form*, and incorrectly recorded the termination "effective date" on the form (See Appendix C for more information).

Per the Council's *Technology Governance Policy,* the Regional Administrator is accountable for ensure technology security standards are developed and implemented to ensure the timely termination of employees and maintain timely identity management for technology systems. When there are incomplete procedures or policies and inadequate trainings for terminating employees, it increases the risk that managers will fill the forms out incorrectly and risk delaying the employee termination process. Additionally, by not documenting termination submission information, the Council risks being unable to determine who is responsible for the late terminations and pinpoint issues in the submission process, or support audits and investigations. If policies and procedures do not ensure timely terminations, a rogue employee could inappropriately access Council systems or assets after their termination and interrupt Council services or systems. The lack of manager training and accountability are a major contributing factor to timeliness issues. Separate identify management processes in HR and IS has contributed to delays in processing employee terminations and deactivating network access.

Recommendation:

1. HR staff should work to immediately minimize late terminations and document the reason for late terminations to ensure accountability for identity management. Specifically, HR should include a risk-based definition of what constitutes a timely termination and include documentation requirements and data retention schedules required to document the reason late terminations. Managers and HR staff should receive regular trainings to support timely employee terminations. An exceptions process for late terminations should be created and documentation maintained to support any authorized exceptions and mitigate the risk of late terminations.

HR and Payroll staff should work to update policies, procedures, and work instructions to ensure guidance is given to managers regarding who is eligible for paid benefits when the worker reports zero hours worked. Procedures or work instructions should include documentation controls.

Documentation should increase accountability and audits should be performed to ensure benefits eligibility requirements are defined and communicated to management.

Management Response: Management agrees with the observations/recommendations and HR and Payroll will partner to complete the following:

- Human Resources will create a late terminations log to document reasons for the delay (to assist with identity management).
- Human Resources will define a risk-based definition of timely terminations based on the Separations of Employees procedure definition (2 business days) and determine the retention schedule for the data collection on late terminations.
- Human Resources will provide training on completing Leaving Service Forms for supervisors and managers Council wide.
- Human Resources will log any exception reasons to late terminations.
- Payroll will review after each pay period, a report that shows zero hours worked, but a payment made. This information will be provided to the manager that approved the timecard, HR, and the Deputy RA/ CFO. The approval for such pay, must be given by the Deputy RA/CFO.

Timetable: March 31, 2023

Staff Responsible: Marcy Syman (HR Director) and Marie Henderson (Deputy Chief Financial Officer)

Audit Follow-Up: Retest

Managers and IS Staff have not consistently terminated network user accounts in a timely fashion.

The IS Department's process for terminating Microsoft Active Directory (AD) network and Office 365 access has not consistently terminated access in a timely manner. Managers are required to notify IS staff, separate from the HR process, with a second form to disable access and delete the account. When HR staff process the termination, the HRMS system sends an email to the manager of the terminated employee. When the manager hits the link in the automated email, the *Network Access Request Form* is populated with basic employee data to make it easier for the manager to submit the form to terminate network access. The manager is then expected to fill in network access to be terminated based on "user type" and submit the form. Prior to March 2022, the concurrent HR and IS procedures could take as long as 6 days from the effective date of the termination to terminate the employee and terminate their user access. The IS Department has not yet been able to execute any Service Level Agreements with departments and divisions to created contracted expectations of the types and standards of service that could be offered.

Internal Audit observed a discrepancy between the number of employee terminations processed by HR staff in the PeopleSoft HRMS (HRMS) system and service tickets process by IS staff to terminate network access in the Ivanti System. HR processed 948 terminations of individual employees, while IS staff processed only 883 service tickets requesting deletion network access over the timeframe of Jan.1, 2020 to Dec.18, 2021. Every employee termination should have an Ivanti Service Desk Ticket to process the network access termination. The process is highly dependent on the managers submitting the necessary forms to IS, so IS staff can produce a service ticket to terminate the account. Senior management has not established a process to hold the managers accountable for submitting the required form to IS staff to process. Internal Audit additionally reviewed termination activity logs for

Microsoft Active Directory (AD), to confirm if any access had been terminated without the creation of an Ivanti Service ticket. The AD Audit system logs access management activity for network access management but IS Staff have limited activity record retention data for account disablement and deletion to one year. Given the limitations of log data, we were limited to testing the link between HR termination data to IS service ticket data, provided by the Ivanti system. In reviewing a sample of network termination forms, Internal Audit also observed that IS staff did not have *Network Access Request* form to terminate network access for 8 of the 20 sampled employee terminations (40%). Internal Audit additionally observed that the limited amount of AD termination activity data resulted in 5 of the 20 sampled terminations not having an AD Admin account disabled date available. The missing *Network Access Request Forms*, limitations of the Ivanti Service ticket data, and the lack of AD Audit system data together were the result of a fragmented, ineffective control environment. Due to the lack of documentation and communication between HR Staff, IS Staff, and Managers, Internal Audit could not reconcile the number of network accounts disabled to the number of employees terminated.

The IS department did implement automated account disabling in March 2022, that disables and later deletes network accounts based on the employees last day worked. Currently, IS does not document the disabling and deletion of accounts on all Council network domains. For those domains where automated terminations are documented, no quality assurance testing is performed on the script for account disabling and deleting to confirm the script is deleting all expected network accounts. The council hosts approximately 9 network segments, including environments hosting services for industrial control systems, payment card data processing, as well as criminal justice information systems, in addition to other division specific information systems.

Disabling inactive and terminating accounts, as supported by NIST and CIS (Center for Internet Studies) standards, would limit unauthorized access to assets or data and provide increased information security and privacy. As a part of the Technology Governance Policy, the ESPT was tasked with commissioning the development of Technology Security Standards, including standards that would include standards related to termination of network accounts. The IS department's requirement of a second form to terminate network access added complexity that often-prevented managers and IS staff from working in tandem to complete timely terminations.

Without defined responsibility and accountability to manage IS network access, network termination processes fail to ensure timely access terminations for higher risk for potentially disgruntled vendors and employees. Failure to audit automated account termination processes may prevent the IS department from identifying issues with automated processes, unintentionally failing to terminate certain network accounts. By limiting AD log data retention to one year from the date of the query, IS limits their ability to monitor deletion and disablement activity, which may reduce the effectiveness of logs to support audits or investigations. When managers and IS Staff consistently fail to ensure that terminations and access disabling is timely, Council networks, databases, and applications could be compromised affecting the confidentiality, integrity, and availability of data and systems.

See Appendix B for more information

Recommendation:

1. The IS department should execute a service level agreement with Council divisions that clearly establish a risk-based timeliness metric and terminate access in a timely fashion when an employee leaves the Council. The IS Department should document in the SLA any exceptions processes and document the justification for any terminations that are not executed in a timely fashion. When

possible, the Council’s IS Department should explore the use of automated access disabling tools across all the network domains.

Management Response: Management agrees with the observation and thinks that a more expansive strategy would be needed to realize a long-term resolution to the risk identified. The Council uses hundreds of applications, some of which are managed by the central IT Department and others outside of the purview of central IT. To comprehensively apply identity access management standards across a distributed IT environment requires a significant initial project and an ongoing program to sustain the results. To fully realize the risk reduction benefits of IAM, the effort must at least apply to all systems that are essential to Council operations or contain non-public data. The initial project would require inventorying all applications and implementing a technical tool to manage access in those apps, as well as creating procedurally supported technical standards. The ongoing program would continuously enroll new applications into the use of the tool and ensure compliance with standards as well as maintain the required technical infrastructure.

Timetable: Before IAM can be realized, a technical foundation of Single Sign On (SSO) and Multi Factor Authentication (MFA) must be achieved. SSO and MFA will be implemented for all technically compatible public facing systems or systems which contain non-public information by the conclusion of 2023. A full IAM program will be presented for consideration in the Council’s 2024 budget planning, during which it will be weighed against other cyber security improvements from a cost/opportunity to risk mitigation ROI perspective.

Staff Responsible Gretchen White (Director, Operations, and Infrastructure)

Audit Follow-Up: Assess Risk

Conclusions

Effective implementation of user administration controls, including the secure and timely management of a users' identity and account access, is a critical component of any organization's information security program. The Council must be able to provision, transfer, and terminate employee's system access as a part of an Identity and Access Management program. User administration is a critical function to secure organization assets while facilitating the use of technology systems of the organization. Technology Security frameworks offer standards and best practices that provide methods to ensure the various components of user administration are integrated into the control environment. Implementing identity and access controls for employees help ensure the appropriate restrictions to the Council's data and assets. Identity and access controls are ideally included as a part of an Identity and Access Management program. Effective user administration enables an organization to audit and report on identity and access management to maximize value and secure public assets while providing necessary public services.

December 9, 2022
Matthew J. LaTour, Director Program Evaluation & Audit
Chief Audit Executive

Appendix A

Program Evaluation and Audit recommendations are categorized according to how Audit will follow-up on them. The categories are:

- **Retest** — Audit will retest the area using the same or similar procedures after a recommendation has been implemented and sufficient time has passed for the changes to take effect. The retest will take place on a specified timetable. The recommendation will be closed once the change has occurred. A new audit project will be opened for retesting and any new findings will include new recommendations
- **Confirmation** — Audit will confirm that an adequate risk response has been completed on the agreed upon timeline. The recommendation will be closed once the change has taken place.
- **Assess Risk** — Audit will not plan for specific follow up to these recommendations. Audit will discuss the area as part of its annual risk assessment activities and consider future audit work in the area.

Distribution List

All audit reports are reported to the general public and are available on *www.metrocouncil.org*. This audit report was distributed to the following parties:

- Members of the Audit Committee
- Regional Administrator
- General Manager/Division Director
- Department Director
- Process Manager

Appendix B: Additional Issue Details

Observation 1: The Council currently has various policies and procedures for user administration that are not informed by industry standards or best practices.

At present, the process for a termination is based on an employee's manager who has the responsibility of initiating the termination and performing follow ups on the termination process. In total the Council has over 475 managers and supervisors across all divisions. Currently there are no Service Level Agreements (SLAs) between the Divisions, HR, and IS to document expected service levels for employee terminations. The HR Procedure notes a preference, but not a requirement, that employees give 2 weeks' notice. Managers currently have 2 days to submit a leaving service form (per HR guidance in HR 7-1l *Separation of Employment Procedure*). HR staff states, the HR director now follows up with managers when the *Leaving Service Form* is submitted late, but accountability has not been applied consistently. HR Assistants have stated they have 1 day to process the form. Per IS staff, the manager should submit an IS *Network Access Request Form* service request to terminate network access. Thought it is not documented in procedure, the IS service desk states that it could take up to 3 days to process the service request to disable the account. In total, current processes can take up to 6 business days after an employee is terminated to complete the termination process. Internal Audit observed that for both the HR and IS process, multiple requirements stated in interviews were not documented requirements and no point in the process is mediated by an SLA. Additionally, the Council does not have any policy or procedure around emergency terminations, which could result in theft or damage of assets or data.

The Technology Governance Policy requires the Council's senior management, the Enterprise Services Planning Team (ESPT), to create and implement technology security standards. Effective technology security standards would address identity and access management and be informed by NIST or CIS control guidance. Procedures or work instructions should note how the mix of automated and manual controls mitigate risk and support the business process for user terminations. Generally, guidance states organizations should limit access to physical assets and systems based on least privilege needed by their position. Guidance also states organizations should consistently ensure timely terminations, where timeliness is defined and based on the risk associated with the user account.

The current HR *Transfer Procedure*, HR 7-1e, does not provide information on how to use the *Personnel Action Request* (PAR) form to process employee transfers to new positions and corresponding access review requirements. There are no policies or procedures requiring quality checks around employee transfer actions that are conducted for the completed PAR forms, which are manually entered. Additionally, relevant HR procedures including the HR *Employees in the Workplace Procedure*, HR *New Employee Orientation and Onboarding Procedure*, HR *Transfer Procedure*, have not been reviewed in 2 years, outside of the *Inactive User and Vendor Account Management Procedure*.

Without effective user administration procedures or technology standards, controls may fail to termination employees in a timely fashion. When HR staff do not follow effective technology security standards, there is a greater risk that terminated employees may access and damage Council systems or receive improper paychecks or other benefits.

Observation 2: The Council has not implemented Role Based Access Controls (RBAC).

Oracle, the company that develops the PeopleSoft software, has created the system components to implement RBAC. Permission lists exist in PeopleSoft Financial and HRMS and can be compiled into user roles. Microsoft has also created functionality such that access detail names can be mapped to specific drives on an Active Directory network. However, roles in all these systems lack documentation or descriptions regarding the access associated with the role. As managers and supervisors find it difficult to understand the roles available to assign to employees, they generally chose to assign access based on another employee in the office, designated as the "Employee to be modeled" after on access request forms.

Roles do not confirm separation of duties in access provisioning for PeopleSoft Financials by identifying the read/write access by field and table associated with the role. Roles in PeopleSoft HRMS appear to be tracked to the field and table level, though Separation of Duties are not clearly articulated and documented. For network access, a number of application and network "Access Details" roles exist, and the names of the network drives employees can access are available. However, Access Detail names are not matched to an access description or other details that establish the business need for the role to access the drive.

Additionally, there are no reviews to confirm that role access establishes separation of duties (at the data field and tale level), or that roles are based on the least privilege required for the associated business need for a position within the organization. Though AD admin is a tool that provides some reporting options that could support RBAC reviews, the IS Infrastructure group has only implemented ad hoc reviews of administrative accounts.

NIST Guidance states that given the risk and criticality associated with the system or hardware, access should be based on roles restricting system access to authorized users, based on business need and separation of duties. Periodic Access Reviews should be conducted to review the access associated with a role, and the roles assigned to individuals. RBAC should ensure roles are based on the principles of least privileged for a given business purpose and separation of duties. Role access and role assignment should also be periodically confirmed by data and system owners. Data owners should be identified as the business owner of data. Data owners should be empowered to determine who is allowed to access the data and system owners should restrict access, as directed by data owners, to the systems they administer.

Observation 3: Manager, HR, and IS processes resulted in a large number of late employee access terminations.

HR processing delays included termination classification issues, which in turn increased the time it took to process terminations. HR processes a higher percentage of late terminations for certain termination reason code categories processed. Reason codes are used by HR Assistants in processing HRMS system entries to record the reason for each termination at the Council. Currently, the HRMS system has 24 active reason codes that HR Assistants can select, though only one reason code may be entered for each termination. There were 6 reason codes in which the late termination rate was especially high. The "End Miscellaneous Driver" (EMD) reason is used to terminate employees bus driver position when the individual had a primary job and became a part time bus driver in addition to their primary job. Reason code categories describing reasons for firing an employee are important to note because they may increase the risk associated with a delayed termination of a potential "rogue" employee, i.e., a possibly hostile employee who could use their access to damage Council systems or assets. In the nearly 2-year cycle, 8 out of 8 terminations (100%) of miscellaneous bus driver position were not terminated on time. The latest termination in this category was 116 days late, and on average, terminations were late by about 20 days. HR additionally processed several late terminations by reason type, including:

- 1 out of 7 terminations in the “Job Abandonment” category
- 9 of 22 terminations for “Unsatisfactory Performance”
- 3 of 10 terminations for “Violation of Rules”, and
- 2 of 6 terminations for employees who “Failed to Show” category (See 5.1.7).

Per the Technology Governance Policy, the ESPT should commission the development and implement controls to ensure employee terminations and access terminations, supported by NIST and Center for Internet Studies (CIS) best practices. Specifically, procedures and technology security standards should ensure that employee terminations are processed timely to prevent erroneous pay and ensure access to Council assets is limited.

The lack of an Identity and Access Management program, definition of what constitutes a timely termination and requirements for staff training have contributed to the delay of terminations and added confusion what forms and information are needed to carry out a termination. Reason code determinations need to be linked to employment contracts. While managers do receive an initial training when hired as a manager, no specific training is provided through Learning and Organizational Development for managers or HR Assistants on how to apply employment contract requirements to termination reason coding. Furthermore, policy and procedures did not inform HR processes and confirm retention requirements for communications via email.

When there is no training and incomplete procedures or policies for terminating employees, it increases the risk that managers will fill the forms out incorrectly and risk delaying the employee terminations process. Additionally, by not linking the process and procedure to a defined business need to document termination submission information, the Council risks being unable to determine who is responsible for the late terminations and pinpoint issues in the submission process. If policies and procedures do not ensure timely terminations, a rogue employee could inappropriately access Council systems or assets after their termination and interrupt Council services or systems.

Observation 4: IS Staff and Managers have not consistently terminated network access in a timely fashion.

For vendor access to Council systems, we observed there were no system controls that exist to prevent IS Staff from entering an access end date exceeding 180 days for vendor network accounts. Though it is not documented in the Tech 2-1h *Inactive User and Vendor Account Management procedure*, 180 days was established by IS Infrastructure Department as acceptable time frame within which to terminate vendor accounts. Further, IS department management has not specified tasks or defined network terminations as the primary duties of any specific IS staff; duties are shared among a group of IS staff. Additionally, there is no policy or procedure documenting requirements for emergency network terminations.

The IS department did implement automated account disabling in March 2022, that disables and later deletes network accounts based on the employees last day. Currently, IS does not document the disabling and deletion of accounts on all Council network domains. For those domains where automated terminations are documented, no quality assurance testing is performed on the script for account disabling and deleting to confirm the script is deleting all expected network accounts. The council hosts approximately 9 network segments, including environments hosting services for SCADA

(Supervisory control and data acquisition) systems, Payment Card Industry Data Security Standard (PCI DSS), Criminal Justice Information Services (CJIS) compliance, as well as general Council staff computing.

IS processes and procedures were not tied together in a documented Identity and Access Management Program. The IS department's requirement of a second form to terminate network access added complexity that often-prevented managers and IS staff from working in tandem to complete timely terminations. Additionally, the IS Infrastructure Department established 180 days as an acceptable time frame for vendor account access, though the timeline is not required by the procedure.

Without defined responsibility and accountability to manage IS network access, network termination processes fail to ensure timely access terminations for higher risk for potentially disgruntled vendors and employees. Failure to audit automated account termination processes may prevent the IS department from identifying issues with automated processes, unintentionally failing to terminate certain network accounts. By limiting AD log data retention to one year from the date of the query, IS limits their ability to monitor deletion and disablement activity, which may reduce the effectiveness of logs to support audits or investigations. When managers and IS Staff consistently fail to ensure that terminations and access disabling is timely, Council networks, databases, and applications could be compromised affecting the confidentiality, integrity, and availability of data and systems.

METROPOLITAN
COUNCIL

390 Robert Street North
Saint Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org