MEMORANDUM OF TRANSMITTAL

To: Rosa B Akhtarkhavari, Deputy Chief Financial Officer

From: George J. McGowan, CPA
Director, Office of Audit Services and Management Support

Date: May 2, 2024

Subj: Microsoft 365 Inactive Accounts (Report No. 24-03)

The Office of Audit Services and Management Support has performed a review of the Microsoft 365 Inactive Accounts. The audit objectives were to assist Information Technology Department to identify a solution for limiting the number of inactive Microsoft 365 accounts maintained by the City.

We conducted this performance audit in conformance with the International Standards for the Professional Practice of Internal Auditing. 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 City's Microsoft Enterprise Agreement, which is a comprehensive contract for all the Microsoft licenses needed for the City, is coming up for renewal in June 2024. In preparation for the contract renewal, Information Technology (IT) would like to review the current 365 licenses. This could reduce the direct license costs incurred, but more importantly would reduce the risk of inactive accounts being used inappropriately by either current less-sophisticated users or by bad actors (through phishing or other cyber-attacks). We have been informed that IT has made attempts to persuade the City's Divisions and Departments to relinquish inactive 365 accounts that have not been accessed in the last six (6) months or more. IT commissioned ASMS to help identify a solution for this matter.

The scope of this review focused on the Microsoft 365 inactive email accounts with no log in for six (6) months (as of April 2024) or more. After several conversations, ASMS and IT agreed on the following objectives:

1. Help Divisions understand why 365 accounts should not left "open" and active after their users are no longer utilizing them.
2. Have business units create a justification for having a 365 account active beyond a reasonable timeframe.
3. Help the Divisions understand the cost associated with each 365 account, and
4. Recommend solution(s).

Current City Practice

We were informed by IT security that the current practice for controlling Microsoft Active Directory accounts (and therefore, email accounts) is to disable the account for two weeks after IT learns of an employee termination through either: a Workday termination notification; an email from a terminating manager; or after an IT Security audit.

During this two week period, IT provides delegated email access to managers who request it for their terminated employees. This access may, with additional justification and director approval, be extended to six weeks.

It should also be noted that after accounts are disabled, the email history for the accounts is retained in accordance with Florida public records requirements.

Best Practice Research

We searched for best practices as well as specific language speaking to the industry time frame for deleting Microsoft 365 inactive accounts, but there is no industry consensus that we could find. Therefore, we surveyed what other organizations are doing about Microsoft 365 inactive accounts. We noted that most organizations are more concerned about the security aspect of inactive accounts, rather than the possible cost savings. Inactive accounts are more susceptible to be compromised, as most use old passwords and may not have two-factor authentication (2FA), making them a more likely cyberattack threat. Additionally, a breach to any service may allow a bad actor access to business accounts and/or the network. Our research showed that suggested inactive account deletion times range from 45 days (Defense Logistics Agency) to 2 years (Google).

We also reached out to our audit co-source partners for their expertise and experience regarding how each of them advises clients regarding inactive accounts. Discussion with these peers revealed the following:

- Carr, Riggs, & Ingram: There is no specific authoritative guidelines. Best practices suggest deleting inactive account after 6 months to 2 years of inactivity. However, they suggest that IT should consider whether deletions may cause issues with other systems/applications that are integrated with the user.
- RSM: Set-up an Inactive account group to block login; ensure the inactive account is a part of the backup retention as per Sunshine Law and delete the account after 30 days. This will give IT an additional 30 days to recover the data if needed.
- CBIZ: Contractual and regulatory obligations should be considered before deleting accounts. Depending on the account type (Admin vs. non-Admin) the inactive times should be shorter/longer. Also, there should be a business rationale to keep accounts longer/shorter than time specific. Payment Card industry (PCI) requires 90 days, and the Center for Internet Security (CIS) suggests 45 days. CBIZ Pivot Point Team believes that 6 months to 2 years is longer than what they normally encounter.

- Clifton, Larson, & Allen (CLA): Microsoft CIS or 365, CISA or NIST do not have an exact prescribed timeframe for retaining inactive accounts. For on premise Active Directory accounts, it's generally 30 to 90 days (for non-privileged and non-service accounts). In some instances, it may be up to 2 years. CIS Critical Controls v8, Control 6.2 recommends establishing an access revoking process and follow it. Also, CIS recommends disabling accounts instead of deleting to preserve the audit trail. CLA suggests that IT take certain factors into consideration such as, risk associated with deleting/retaining the account for longer/short period, retention should be based on roles and responsibility, and a justification for longer retention periods for inactive accounts.

Review of City 365 Accounts

We learned that the City uses two types of licenses for Microsoft 365 accounts: G1 – with 50GB Mailbox storage with 1TB OneDrive storage, and G3 – with 100 GB Mailbox storage with unlimited OneDrive storage. These have an annual cost of about $64.04 and $286.01 respectively, for each license. We used this information and the Inactive Accounts report (as of 4/3/24 which was provided by IT) to determine the direct cost of keeping licenses for these inactive accounts. In total, we found 98 inactive accounts (there are about 3,784 G1 and G3 accounts so the inactive accounts are about 2.5% of the total). We identified the departments with the largest number of inactive accounts, See **Schedule I** attached.

Our review of the inactive accounts revealed the following:

- The total annual cost for the 98 inactive accounts is $6,942 ($6,084 for G1 and $858 for G3). An examination of the last vendor invoice revealed that overall total annual cost was $708,686 ($107,779 for G1 and $600,907 for G3). Because the number of inactive accounts may change from time to time, so, the direct cost impact of continuing to carry these licenses will vary throughout the year.
- Three departments, Public Works, Families Parks and Recreation, and Venues have the most inactive accounts; the number of inactive accounts is 58, 18, and 17 with an annual cost of $3,936, $1,375, and $1,311 respectively.
- Inactive time frames for the 98 accounts are: Less than 6 months: 9 accounts (at a cost of $576 annually); 6 months to 1 year: 23 accounts ($2,139); 1 to 2 years: 22 accounts ($1,409); 2 to 3 years: 17 accounts ($1,089); 3 to 4 years: 5 accounts ($320); 4 to 5 years: 13 accounts ($833); 5 to 6 years: 7 accounts ($448) and 6 to 7 years: 2 accounts ($128).

Conclusion

Based on the research conducted and review of inactive accounts, ASMS concludes that:

- The current practices of the IT security section go above the account deletion timelines suggested by most best practices.

- Despite these efforts, some departments continue to have open and inactive accounts increasing the exposure of the City to possible cyber-attacks.

Therefore, we suggest that:

IT notify affected departments every quarter of the accounts that have been inactive for more than thirty days with notice that IT intends action to disable the account unless the department provides justification for keeping the account active within two weeks of receiving the notice.

This justification should include an acknowledgement of the department's acceptance of the increased risks to the City of keeping the account.

IT has concurred with this suggestion.

c: Jody Litchford, Deputy City Attorney
Kevin Edmonds, Chief Administrative Officer
Michelle McCrimmon, Chief Financial Officer

Schedule I

Inactive Microsoft 365 Accounts By Department (as of 4.3.24)

Department	< 6 Mon.		> 6 Mo.		1-2 Yrs		2-3 Yrs	
Public Works	4	$ 256.16	13	$ 1,054.49	11	$ 704.44	9	$ 576.36
Families Parks And Recreation	2	128.08	6	606.21	6	384.24	4	256.16
Orlando Venues	2	128.08	2	350.05	5	320.2	3	192.12
Economic Development	1	64.04					1	64.04
Police			1	64.04				
Business and Financial Services			1	64.04				
Sub Total	**9**	**576.36**	**23**	**2,138.83**	**22**	**1,408.88**	**17**	**1,088.68**

Department	3-4 Yrs		4-5 Yrs		5-6 Yrs		6-7 Yrs	
Public Works	4	$ 256.16	10	640.4	5	$ 320.20	2	$ 128.08
Families Parks And Recreation								
Orlando Venues			3	192.12	2	128.08		
Economic Development								
Police	1	64.04						
Business and Financial Services								
Sub Total	**5**	**320.20**	**13**	**832.52**	**7**	**448.28**	2	**128.08**

Department	Number	Yrly Cost
Public Works	58	$ 3,936.29
Families Parks And Recreation	18	1,374.69
Orlando Venues	17	1,310.65
Economic Development	2	128.08
Police	2	128.08
Business and Financial Services	1	64.04
Grand Total	**98**	**6,941.83**