REPORT OF EXAMINATION | 2021M-215

City of Lackawanna

Network Management and Internal Controls

APRIL 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

City of Lackawanna

Audit Objective

Determine whether City of Lackawanna (City) officials properly implemented information technology (IT) security controls to safeguard the network against unauthorized access or disruption.

Key Findings

City officials did not establish adequate controls to safeguard the network against unauthorized access or disruption.

- City officials did not regularly review, identify and disable unnecessary network user accounts. As a result, 14 unnecessary generic network user accounts and 26 usernames associated with inactive or former employee accounts were not disabled.
- City officials have not developed written IT policies and did not provide users with IT security awareness training.
- City officials have not developed a written IT contingency plan.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop written policies and procedures for managing network access and disable unnecessary network user accounts.
- Provide periodic IT security awareness training to all personnel who use IT resources.
- Develop a comprehensive written IT contingency plan.

City officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The City is located in Erie County and is governed by an elected Mayor and an elected five-member City Council (Council). The Council is responsible for the general oversight of City operations and finances. The Mayor is responsible, along with other officials and staff, for managing day-to-day operations.

The Mayor hired an IT Specialist (Specialist) in August 2020, shortly before our audit began, to oversee IT security and manage the City's IT operations. Prior to this appointment, the City relied on the purchasing agent with the help of a third-party vendor to provide IT support for the City's network.

Quick Facts	
IT Budget 2020-21	$138,300
Number of Computers	44
Network User Accounts as of March 31, 2021	89

Audit Period

August 1, 2020 – September 7, 2021

Network Management

How Should Officials Manage Network User Accounts?

Network user accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users. These accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access, and view data stored on the network. Therefore, network user accounts should be actively managed and periodically reviewed to minimize the risk of unauthorized access or misuse.

Because generic network user accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network and applications. If generic network user accounts are needed (e.g., for certain network services or applications to run properly), officials should have procedures in place to monitor who uses the accounts and when they are used.

A city should have written procedures for granting, modifying and revoking access rights to the network. To minimize the risk of unauthorized access, officials should regularly review enabled network user accounts to ensure they are still needed. Officials must disable unnecessary or unneeded network user accounts as soon as there is no longer a need for them, including network user accounts of former employees or employees who have transferred to another area.

City Officials Did Not Adequately Manage Network User Accounts

City officials did not actively manage network user accounts and the City did not have procedures in place for granting and revoking access rights to the network. We reviewed all 89 of the City's enabled network user accounts and found 35 were assigned to current employees, 23 were generic network user accounts (not assigned to a specific user), 26 network user accounts were associated with former employees and five default network user accounts were administrative user accounts associated with specific software.

Unneeded Generic Network User Accounts – Of the 23 generic network user accounts that we identified, nine were necessary for City operations and actively being used to perform various administrative functions. However, the remaining 14 generic network user accounts had not been used in at least six months, and three had elevated administrative permissions. The Specialist told us that these user accounts were unneeded and would be disabled and immediately removed the three user accounts with elevated administrative permission.

City officials had not been reviewing and disabling unnecessary generic network user accounts. Unnecessary generic network user accounts expose the City to

a greater risk that personal, private and sensitive information (PPSI)[1] could be changed intentionally or unintentionally or be used inappropriately, and officials may not be able to identify who performed the unauthorized activities.

Unneeded Network User Accounts – We identified 22 enabled network user accounts that as of March 31, 2021 had not been used in the last six months and were not associated with current active employees and therefore, were unneeded and should be disabled. We also identified four enabled network user accounts that had been used within six months but were no longer associated with current active employees and therefore unneeded. Two of the four accounts were previous City Clerk accounts being used by the current City Clerk. This occurred because City officials had not established a process or written procedures for revoking network access immediately upon termination or resignation of an employee.

The Specialist confirmed that these network user accounts were assigned to former employees that had not been disabled from the network access upon resignation. At the time we conducted our audit testing, the Specialist had been in his position for approximately six months and much of his initial duties focused on supporting the City's efforts to continue operating remotely during the COVID pandemic, assisting with a major software change and updating user operating systems. As a result, he indicated to us that he had not had an opportunity to review network user accounts.

When officials do not ensure unneeded network user accounts are disabled, there is a greater risk that these user accounts could potentially be used by former employees or others for malicious purposes. Revoking access to employees who leave service helps to ensure that their network user accounts are not accessible to alter, delete or otherwise damage data or programs.

Why Should a City Have Written IT Policies and Security Awareness Training?

A well-informed work force is essential to helping to secure a network from unauthorized access or disruptions. Written IT security policies define a city council's expectations for appropriate user behavior, describe the tools and procedures needed to protect network resources (e.g., data, files) and explain the consequences of policy violations. A city council should provide important oversight and leadership by establishing written policies that take into account people, processes and technology. While IT security policies will not guarantee the safety of the network, a lack of appropriate policies significantly increases

1 Personal, private and sensitive information (PPSI) is any information to which unauthorized access, disclosure, modification, destruction – or disruption of access or use – could have or cause a severe impact to critical functions, employees, customers, third parties, or other individuals or entities.

the risk that data may be lost or damaged by inappropriate access and use. In addition to IT policies defining the city council's expectations for computer users, IT security awareness training will help provide city officials and employees with the skills to do it.

The training should center on current and emerging trends such as information theft, social engineering scams and computer viruses and other types of malicious software (e.g., ransomware), all of which may result in PPSI compromise or denying access to the IT system and its data. Training programs should be directed at the specific audience (i.e., network users or administrators) and include information attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections, or how to respond if a virus or an information security breach is detected.

City Employees Were Not Provided with IT Policies or IT Security Awareness Training

The Council and City officials have not developed and adopted written IT policies and officials did not provide users with IT security awareness training to help ensure they understand IT security measures designed to help safeguard the network from potential unauthorized access or disruption. As a result, IT assets and data could be more vulnerable to loss and misuse. The Specialist stated that in the future he would like to provide IT security awareness training to City employees, however, due to current COVID-19 pandemic precautions in place, he has not been able to. The former City Comptroller indicated that prior to the Specialist being hired IT training was not something officials had discussed but they would consider going forward.

City officials cannot be assured there is adequate protection of the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. For example, without such critical training, employees may not understand how their Internet browsing could cause their computers to become infected with malicious software or they may be fooled, via social engineering scams, into providing their passwords, opening harmful attachments or visiting malicious websites. As a result, City data could be at a greater risk for unauthorized access, misuse or abuse.

Why Should the City Have a Written IT Contingency Plan?

IT contingency planning involves analyzing business processes in the event of a disruption and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. As part of the contingency planning process and to minimize the risk of network access disruption, data loss or suffering a serious interruption of services, officials should establish a formal written IT contingency plan (plan) that includes guidance on systems recovery.

The IT contingency plan should address the potential for sudden, unplanned events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the IT system and data. This is particularly important given the current and growing threat of ransomware attacks. In addition, the IT contingency plan should be periodically tested and updated to ensure key officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

City Officials Did Not Have a Written IT Contingency Plan

The Council and City officials did not develop and adopt a comprehensive written plan to describe how officials would respond to potential disruptions or catastrophic events. Consequently, in the event of a catastrophic event or network compromise, officials have no written guidelines or guidance to minimize or prevent network access disruption or loss of equipment and data. While officials acknowledged they did not have a plan, they believed that their current unofficial procedures of preparing multiple backups throughout the week was sufficient.

Without a formal written plan, officials cannot ensure that in the event of a disaster they would be able to restore network access, critical IT systems, applications or data in a timely manner. Depending on the severity of an incident, officials may need to expend a significant amount of time and financial resources to resume City operations. Furthermore, essential employees may not be aware of their roles which could complicate the City's ability to recover from an incident. As a result, the City has an increased risk that it could lose important data and suffer serious interruption in operations.

What Do We Recommend?

The Mayor and City officials should ensure that the IT Specialist:

1. Disables unneeded and/or dormant network user accounts identified during our audit and periodically review network user accounts to identify unneeded or dormant accounts.

2. Restricts the use of generic network user accounts and develop written procedures to monitor the use of these accounts.

3. Develops written procedures for managing network access that include periodically reviewing network user accounts and disabling user accounts when access is no longer needed for the network.

4. Provides periodic IT security awareness training to all personnel who use IT resources that includes guidance on the importance of appropriate computer use.

The Council and City officials should:

5. Develop and adopt comprehensive written IT security policies to define appropriate user behavior and explain the consequences of policy violations.

6. Develop and adopt a comprehensive written IT contingency plan.

Appendix A: Response From City Officials

We redacted certain portions of the response letter due to the sensitive nature of the information. City officials reference two additional responses. The first response is related to, and included in, this report. The second response relates to, and is included in, the City's companion report, *City of Lackawanna, Garbage Collection Fees, 2021M-206*.

Annette Iafallo, Mayor
City of Lackawanna
714 Ridge Road - Room 301
Lackawanna, NY 14218
Tel: (716) 827-6464 Fax: (716) 827-6678

March 28, 2022

[redacted] Auditor
[redacted] Auditor
Division of Local Government and School Accountability
295 Main Street-Room 1032
Buffalo, New York 14203-2510

Dear [redacted]

Thank you for very much for taking the time to audit and point out items that need to be corrected. I totally agree with your findings.

The Commissioner of Public Works, Tony DeSantis and our Computer Technician, Gene Olivieri III, have been working to address your concerns, and have completed a percentage of the items.

Attached are the replies from Tony and Gene, please contact me if you have any questions.

Respectfully,

Annette Iafallo
Mayor

City of Lackawanna
714 Ridge Road – Room 307
Lackawanna, NY 14218
Tel: (716) 827-6477

Dear NYS Comptroller's Office,

Response to Network Management and Internal Controls Report:

1. Disables unneeded and/or dormant network user accounts identified during our audit and periodically review network user accounts to identify unneeded or dormant accounts.

IT understands the importance of this finding. A script for this process was in the works before the audit period began. This script was being developed to identify unused user accounts so they could be disabled and later deleted. The list of network user accounts was reviewed. From the review, the use of each account was identified and 53 unneeded user accounts were disabled. The same routine will be followed when someone leaves City Hall. Their account will be disabled and if that account is not re-enabled within one month the account will be deleted.

2. Restricts the use of generic network user accounts and develop written procedures to monitor the use of these accounts

IT understands the importance of this finding. Action was quickly taken to make sure that the unnecessary generic accounts were disabled. The generic user accounts that are still being used have no elevated permissions as they are used for mostly counter computers. These counter computers are used exclusively for third-party programs with individual logins that the employees need to be able to access. In addition to them not having any elevated permissions, I am currently testing having the generic computers not apart of the domain.

3. Develops written procedures for managing network access that include periodically reviewing network user accounts and disabling user accounts when access is no longer needed for the network.

A written IT security policy is being developed. The plan for keeping the network user accounts list up to date will be included in that policy. This will also include the process when someone leaves City Hall noting that their account will be disabled and if that position or person's account is not filled in one month, that account will be deleted.

4. Provides periodic IT security awareness training to all personnel who use IT resources that includes guidance on the importance of appropriate computer use.

IT understands the importance of this finding. A proper IT security awareness training class will be created using the multiple resources provided by the Office of the New York State Comptroller. This training course is estimated to be developed by the end of 2022.

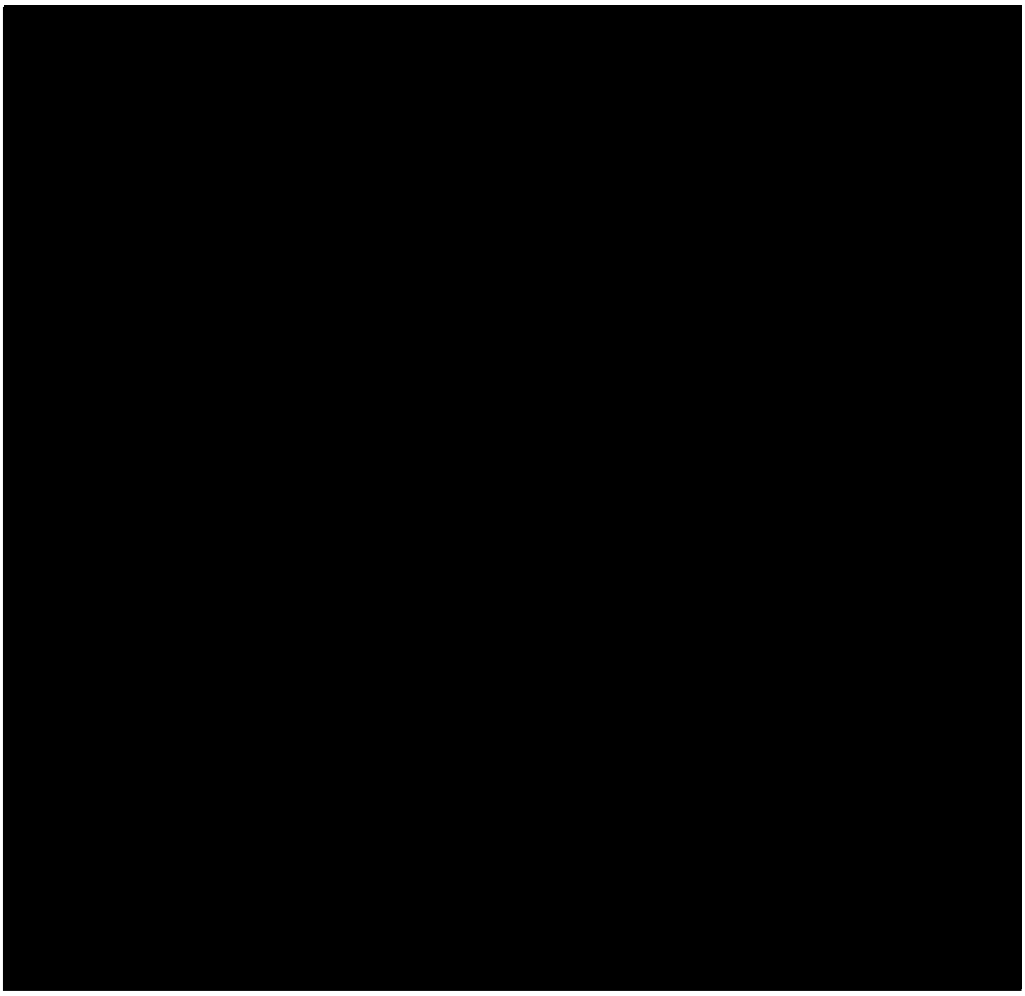
Gene Olivieri III, Information Technology Specialist

5. Develop and adopt comprehensive written IT security policies to define appropriate user behavior and explain the consequences of policy violations.

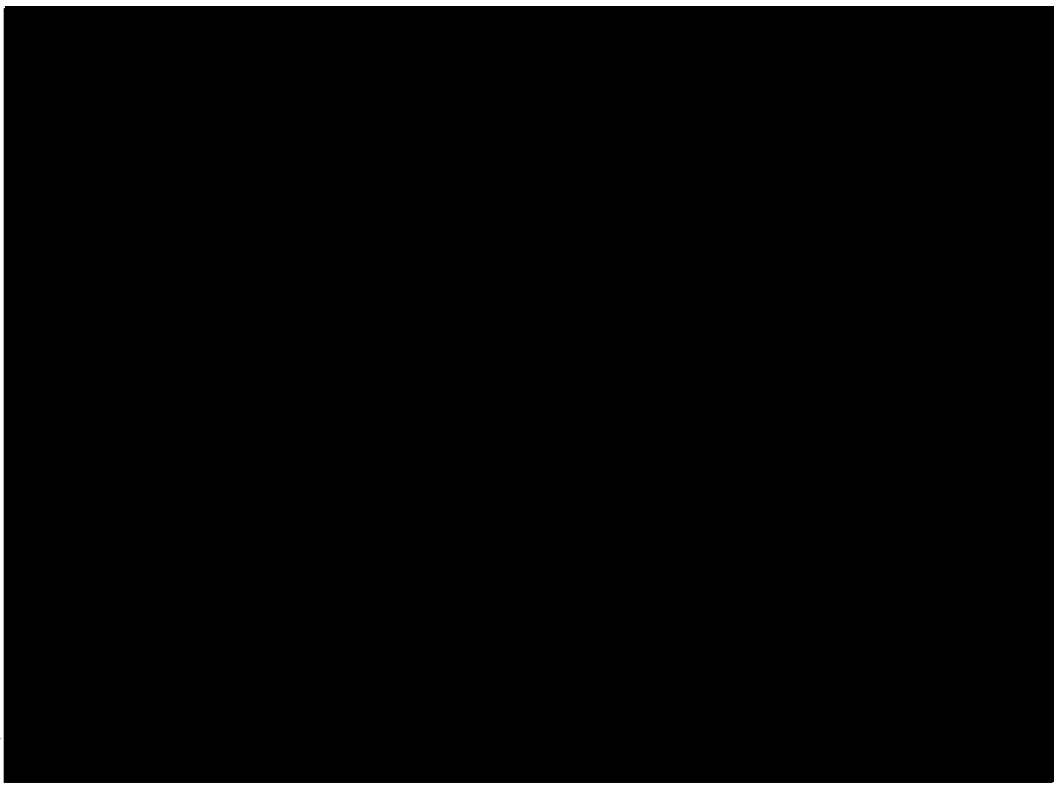
IT understands the importance of this finding. Along with the proper IT security awareness training class, written IT security policies will be developed defining appropriate user behavior and explain the consequences of policy violations. This will be created alongside the training courses noted in #4. The IT security policy will be explained at the IT security awareness training as well. These policies will be put in front of council for review and approval.

6. Develop and adopt a comprehensive written IT contingency plan.

IT understands the importance of this finding. An IT contingency plan will be written by the end of 2022. This plan will be put in front of council to be approved and after that it will be enforced in City Hall starting the day after that City Council Meeting barring it is approved by all.



Gene Olivieri III, Information Technology Specialist



Sincerely,

Gene Olivieri III
Information Technology Specialist

Gene Olivieri III, Information Technology Specialist

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed City officials to gain an understanding of the City's IT operations and reviewed City records for any IT-related policies and procedures.
- We ran a computerized audit script on March 31, 2021 on the domain controller[2] and analyzed each report generated by the script to identify network user accounts and the related security settings applied to the accounts.
- We compared the 89 network user accounts identified by the scripts to a list of current employees to determine whether enabled network user accounts were assigned to current City employees. We interviewed City officials to determine the necessity of generic network user accounts and any user accounts not associated with a City employee.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to City officials.

We conducted this performance audit in accordance with GAGAS (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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The Council has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Council to make the CAP available for public review in the City Clerk's office.

2 The domain controller is a server that controls or manages access to network resources.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

BUFFALO REGIONAL OFFICE – Melissa A. Myers, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller