New York State Comptroller
THOMAS P. DiNAPOLI

Town of Amherst

Information Technology

July 2026 | 2025M-120
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Town of Amherst

Audit Objective

Did Town of Amherst (Town) officials properly secure user account access to the network?

Audit Period

January 1, 2023 – May 1, 2025

Understanding the Audit Area

A computer network is a group of connected computer systems that can communicate with each other, often for the purposes of accessing, sharing, maintaining and managing information stored on connected systems. A town relies on its network for daily business functions, such as maintaining financial records including employees' personnel and payroll records which contain personal, private and sensitive information (PPSI).[1] To minimize the risk of unauthorized network access, town officials must properly secure user account access to the town's network. A secured network can help protect employees' and residents' PPSI, ensure the continuity of essential services and prevent financial losses from cyberattacks.

The Director of Information Technology (IT Director) is responsible for managing the Town's IT resources, including securing network access for 324 network user accounts and 92 network service accounts, managing hardware inventories, and overseeing the IT department composed of five individuals, including the Network Manager, responsible for overseeing the Town's IT hardware and software installations.

Audit Summary

Town officials did not properly secure user account access to the network. As a result, the Town was exposed to an increased chance of unauthorized network access which could cause a variety of disruptions to the Town, ranging from minor operational disruptions to network outages or data breaches.

IT department employees did not disable 11 unneeded network service accounts, two of which had administrative access. Additionally, the IT department did not receive a request to disable network user accounts for three departing employees for more than 30 days after the employee separated from the Town. The IT Director was not aware of the unneeded user and service accounts because he did not require IT department employees to perform a periodic review of network user account access.

Additionally, IT department employees did not maintain an accurate and up-to-date IT hardware inventory list. Specifically, 30 virtual servers out of 272 devices reviewed were not included in the Town's inventory list. Without proper IT inventory records, officials cannot be assured that they are aware of and have properly secured all the hardware that users could use to access the network.

Sensitive IT control weaknesses were communicated confidentially to Town officials.

The report includes five recommendations that, if implemented, will improve the Town's IT practices to secure user account access to the network. Town officials generally agreed with our recommendations, and their response is included in Appendix B.

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

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 (GML). Our methodology and standards are included in Appendix C.

The Town Board (Board) 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 GML. 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 Board to make the CAP available for public review in the Town Clerk's office.

Information Technology: Findings and Recommendations

A town board should adopt comprehensive written policies and procedures that set forth guidelines for periodically reviewing network user account access, disabling network user accounts, and establishing and maintaining IT asset inventories. The town board should periodically review IT policies, update them as needed and establish who is responsible for monitoring compliance with these policies. IT officials should ensure that currently enabled network user accounts are necessary, and unnecessary accounts are removed in a timely manner. The process to disable unneeded accounts should be documented to ensure the timely and appropriate removal of unneeded accounts.

An IT director should ensure IT department employees maintain a detailed, up-to-date inventory of all IT hardware on the network to help properly secure network user account access. Proper IT inventory records are not only critical for protecting hardware from loss, theft or misuse but also for helping to mitigate unauthorized access to the network. Without proper IT inventory records, officials cannot be assured that they are aware of and have properly secured all the hardware that users could use to access the network.

More details on the criteria used in this report, as well as resources OSC makes available to local officials that can help them improve operations, are included in Appendix A.

Finding 1 – IT department officials did not properly remove unneeded network user and service accounts.

The IT Director did not ensure that administrative access granted to two service accounts was needed, enabled network accounts were necessary, and unnecessary accounts were removed in a timely manner.

Administrative Network Access – Administrative access to the Town's network was not properly restricted because two of the 92 network service accounts were granted unnecessary administrative access. The Network Manager stated that there was no business justification for the two accounts having administrative access and the accounts were no longer being used. After our audit inquiry, we observed that the Network Manager disabled the accounts.

Administrative accounts are common targets for attack because of their elevated access. Their compromise allows greater damage than with lesser-privileged accounts because these accounts have full control over the network. Ineffective management of privileged accounts increases the chance of unauthorized access to or exposure of sensitive Town data, including employee and resident PPSI, if the privileged account is compromised.

Network User Accounts – The Board and IT Director did not adopt comprehensive written policies and procedures regarding granting, changing and disabling network user account access or performing periodic reviews of network user account access. However, the IT department had informal procedures which required department heads to notify the IT department of an employee's separation by submitting a request to disable the employee's network user account access.

We reviewed a sample of 16 employees who separated from Town employment between March 2023 and September 2024. We determined that requests to disable network user account access for three employees (19 percent) were not submitted to the IT department for 38 to 191 days after the employees separated from Town employment. Although the Town's request system indicated the date a request was submitted to disable the accounts, it did not indicate the date that requests were completed (accounts were disabled). As a result, we were unable to determine the timeliness in which the 16 network user accounts were disabled. The IT Director stated that department heads did not always notify the IT department of an employee's separation, or notify the department in a timely manner.

We also reviewed 92 enabled network service accounts and identified nine service accounts which no longer required access to the Town's network. IT officials disabled the nine network service accounts after our audit inquiry. While these accounts were not granted administrative privileges, ineffective account removal processes could expose the Town to data loss or disrupt Town operations if the unneeded service accounts were compromised by an attacker.

If the Board and IT Director adopted written policies and procedures for granting, changing and disabling network user account access and required IT department employees to perform periodic reviews of user and service accounts with access to the Town's network, the unneeded network accounts may have been identified and disabled sooner. Unnecessary network user and service accounts may expose the Town to unauthorized network access or data exposure.

Recommendations

The Board should:

1. Adopt a written policy that establishes requirements related to granting, changing and disabling network user and service account access. The policy should outline the department heads' responsibilities for notifying the IT department of an employee separation in a timely manner.

2. Adopt written policies that require a periodic review of network user and service accounts to be performed.

The IT Director should:

3. Develop a written policy and formal procedures related to the processes to grant, change and disable network user and service account access.

4. Develop a written policy and formal process to periodically review user account access to the Town's network and remove unneeded access and permissions. Evidence of the review should be documented and maintained.

Finding 2 – IT department employees did not maintain complete IT hardware inventory records.

IT department employees maintained an IT inventory list of certain Town-owned IT hardware, including servers, desktop computers, laptops and cellphones. However, the IT inventory list did not include all devices that were connected to the Town's network. Furthermore, IT department employees did not periodically review or update the IT inventory list to ensure all IT hardware was properly accounted for.

Of the 272 devices identified in the Town's centralized network management tool,[2] 30 virtual servers (11 percent) were not included in the IT inventory list. Furthermore, 29 of the 30 virtual servers (97 percent) last accessed the Town's network within two months of when testing was performed in December 2024. The IT Director stated that the 30 virtual servers were Town-managed devices and acknowledged that there were gaps in their IT inventory process that could be improved upon. However, had the IT Director required IT department officials to perform an inventory of all hardware and periodically review the results and update the inventory list, inventory records would be more complete and accurate.

Because the IT department did not maintain a complete and accurate IT inventory list, IT hardware could be lost, stolen or misused without detection. As a result, the Town was exposed to an increased risk of

2 A centralized network management tool provides a centralized point of network authentication and resource management, which allows users to log onto the network once and gain access to data and applications on the network in accordance with the access and permissions granted to their accounts.

unauthorized network access which could cause a variety of disruptions, ranging from minor operational disruptions to network outages or data breaches.

Recommendation

5. The IT Director should ensure that IT department employees maintain a complete and accurate IT inventory list and periodically review and compare the devices in the centralized network management tool to the IT inventory list and document/resolve any inconsistencies in a timely manner.

Appendix A: Profile, Criteria and Resources

Profile

The Town, located in Erie County, is governed by the elected five-member Board composed of the Supervisor and four Councilmembers. The Board is responsible for the Town's financial activities.

Each elected official and department head is responsible for the execution of Town policies applicable to their department, and department heads report to the Supervisor. The IT Director is responsible for the management of the Town's network used to support business functions. The IT department consists of five employees, including the Network Manager, network coordinator, two support specialists and a clerk-typist. These employees oversee the Town's IT hardware and software installations, manage the network-based telephone system and provide desktop computer and user support.

Criteria

A town board should adopt written policies and procedures relating to managing user account access to the network. These policies and procedures should establish a centralized process for granting, changing and disabling network user account access, maintaining a hardware inventory and performing periodic reviews of network user account access. The head of the IT department should establish a process for IT department employees to identify and remove unneeded user accounts when the accounts no longer require network access. The process to remove unneeded user accounts should be documented to ensure the timely and appropriate removal of unneeded accounts.

Network user accounts can be directly used by employees or other network users to access the network resources required to complete their job duties and responsibilities. Other network user accounts are classified as service accounts, which are non-human accounts that could be used by applications, services, or systems to interact with other systems and resources. Service accounts can be used for automating certain tasks and may be granted elevated permissions or access to sensitive data. All network user accounts, including service accounts, need to be appropriately managed to ensure only accounts with a valid business reason have access to the town's network. Officials should periodically review employee, service and other user account access to the town's network to correct unnecessary user access rights and remove unneeded accounts when network access is no longer needed. Written steps related to performing the review should be documented and evidence of reviews performed should be documented and maintained.

Generally, a designated administrator account has oversight and control of a network with the ability to add new user accounts and change user accounts' passwords and access. A user with administrative access can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. At times, service accounts will require administrative or similar elevated privileges to function correctly. Where possible, granting service accounts administrative access should be avoided and should be restricted to specific areas, as necessary.

IT hardware inventories are an essential component to properly securing user account access to a network, including the PPSI and data therein, because up-to-date hardware inventories enable IT department employees to effectively track and manage the hardware that can connect to the network. IT department employees should maintain detailed, up-to-date inventory records of all computer hardware devices to help safeguard IT assets. The head of the IT department should ensure IT department employees implement effective inventory management processes to ensure that the hardware that is able to connect to the town network is appropriately managed and tracked. Officials should verify the accuracy of inventory records through periodic inventory counts and reconciliations and a review and update of this inventory should be performed bi-annually or more frequently. Without effective inventory management and tracking, IT department employees cannot be assured that unsupported or outdated hardware is replaced and disposed of in a timely

manner, potentially introducing known vulnerabilities and exploits that could be used by an attacker to gain unauthorized access to a network.

Additional Resources

OSC's *Local Government Management Guides,* and other informational resources that are available on OSC's website to help officials understand and perform their responsibilities, include:

- *Information Technology Governance*: https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf
- *The Practice of Internal Controls*: https://www.osc.ny.gov/files/local-government/publications/pdf/the-practice-of-internal-controls.pdf
- *Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders*: https://www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf
- *New York Local Government and School Cybersecurity: A Cyber Profile*: https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-school-cyber-profile.pdf

In addition, local officials can use OSC's website to search for audits, resources, publications and training for officials at: https://www.osc.ny.gov/local-government

Appendix B: Response From Town Officials

The content below is a reproduced copy of the original response letter issued by Town officials, is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[3] and may have included changes to spelling and grammar. The substance of the content was not changed.

Town of Amherst
Amherst, NY
Amherst Municipal Building – 5583 Main Street – Williamsville, NY 14221
716-631-7000 – toainfo@amherst.ny.us – www.amherst.ny.us

Town of Amherst Response Outline to OSC Audit
Information Technology Report
2025M-120

Finding 1 - IT department officials did not properly remove unneeded network user and service accounts.

The IT Department is collaborating with the Amherst Town Board and the Amherst Information Technology Advisory Committee to establish clear requirements for granting, modifying and disabling network user and service account access. The updated policy will define each department head's responsibility, in coordination with the Human Resources Department, to provide timely and official notification of employee status changes or separations.

Additionally, the IT Department is developing written policies, in coordination with the Amherst Town Board and the Amherst Information Technology Advisory Committee, that will mandate periodic reviews of all network user and service accounts.

The IT Department is also creating comprehensive written policies and formal procedures to govern the processes for granting, revising and disabling network user and service account access. These policies will include requirements for regularly reviewing account access to the Town's network and removing accounts or permissions that are no longer needed. All review activities will be fully documented and retained for reference.

Finding 2 - IT department employees did not maintain complete IT hardware inventory records.

The IT Department is committed to strengthening the completeness and accuracy of its IT hardware and software inventories. Efforts are underway to enhance inventory management processes and address areas where certain hardware and software deployments may not yet be fully integrated with the department's existing inventory systems. The IT Department will continue refining these integrations to ensure that all assets are consistently tracked within the Town's robust inventory applications.

Respectfully submitted on behalf of the Town of Amherst by:

Shawn A. Lavin
Town Supervisor
Amherst, New York
Date: May 21, 2026

3 https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule

Appendix C: Audit Methodology and Standards

OSC auditors obtained an understanding of internal controls that were deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of the work on internal controls, as well as the work performed in the audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed Town officials and employees and reviewed Board-adopted policies to gain an understanding of user account access to the Town's network and the processes performed to manage the Town's IT inventory. We reviewed relevant policies, documents and reports related to user account access to the Town's network and IT inventory list.

- We provided a computerized audit script to the Network Manager to run on the Town's network on December 2, 2024 to determine the network's enabled user and computer accounts. We analyzed the script output to determine whether unnecessary accounts were granted access to the Town's network. We discussed any unnecessary accounts with the Network Manager to determine why the accounts had access to the network or whether they should be disabled.

- We used our professional judgment to select a sample of 16 out of 134 network user accounts that were disabled during the audit period to determine whether a request was made to the IT department to disable the network user account and the request was completed in a timely manner. We used our professional judgment to select our sample to include employees from various Town departments, and to include high-risk network user accounts, such as users who separated from Town employment due to retirement, resignation, etc.

- We analyzed each report generated by the script and compared the results to the Town's IT inventory list to determine whether all hardware devices that were connected to the Town's network were appropriately tracked on the IT inventory list. We discussed discrepancies identified with the IT Director to determine why devices connected to the Town's network were not appropriately tracked on the IT inventory list.

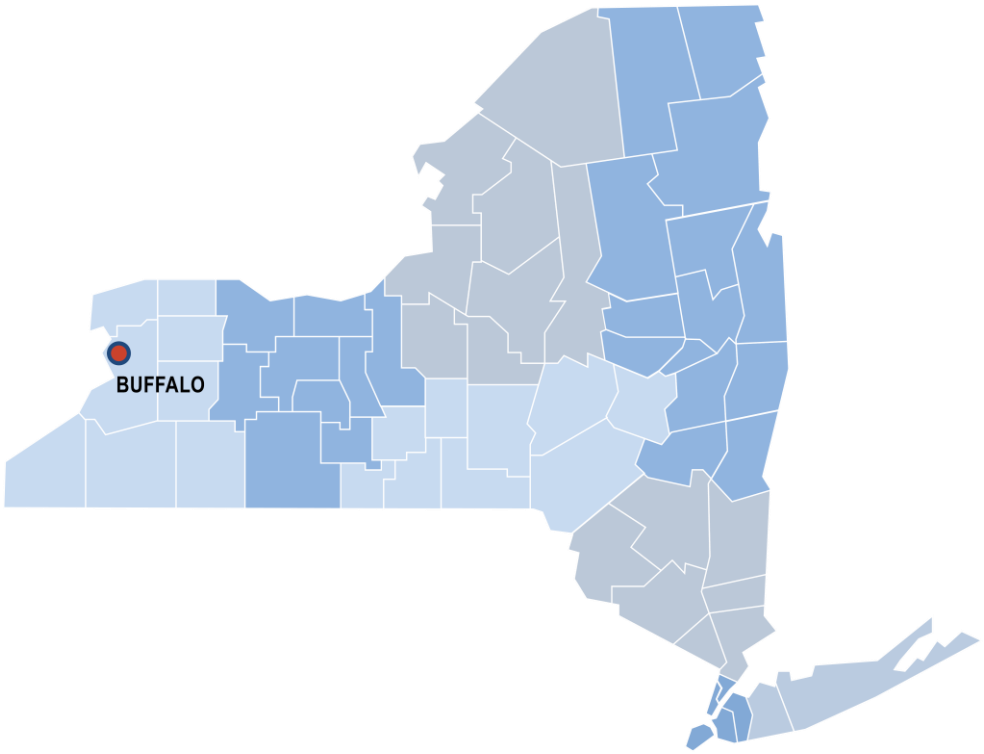
The audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, the results were not discussed in this report, but were instead communicated confidentially to Town officials.

OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected for examination.

Questions?

BUFFALO REGIONAL OFFICE
Melissa A. Myers, Chief of Municipal Audits
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



Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

https://www.osc.ny.gov/

Prepared by the Division of Local Government and School Accountability