New York State Comptroller
THOMAS P. DiNAPOLI

Town of Wilton

Cybersecurity

August 2026 | 2026M – 48
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Town of Wilton

Audit Objective

Did the Town of Wilton (Town) Town Comptroller (Comptroller) adequately safeguard network and cloud-based user account access from cybersecurity threats?

Audit Period

January 1, 2024 – August 8, 2025

Understanding the Audit Area

Adequate user account access safeguards are essential to ensuring that only authorized individuals can access town systems and data. Weak safeguards increase the risk of unauthorized access and activity, data loss, operational disruptions, financial loss, compromise of personal, private or sensitive information (PPSI),[1] and legal and reputational repercussions.

The Town had 56 full-time and 13 part-time employees during the audit period. The Town's network environment consisted of 77 enabled user accounts and 132 computer accounts. In addition, the Town had 110 enabled cloud user accounts which are used for email access. The Town uses a third-party IT vendor to help oversee the IT environment. The Comptroller is responsible for the Town's website, and ensuring the services provided by the IT vendor are performed adequately in accordance with the vendor contract. The Comptroller, along with the IT vendor, is also responsible for establishing controls over network and cloud-based user account access.

Audit Summary

Town officials did not adequately safeguard network and cloud-based user account access from cybersecurity threats. As a result, Town officials cannot be assured that IT systems are secured and protected against unauthorized use, access, manipulation and loss.

The Comptroller did not ensure that user accounts across the Town's network and cloud environments were adequately monitored. We determined that 18 employee accounts and four service[2] and shared accounts were unnecessary and should have been disabled. These accounts exposed the Town's IT assets to an increased risk of unauthorized access, misuse or disruption. Also, the Comptroller did not utilize the IT Vendor to establish and implement a systematic account review process to help ensure that only necessary network and cloud account access remained enabled. The inadequate monitoring and oversight weakened accountability and could lead to difficulties attributing IT system activity to specific individuals.

Furthermore, the Comptroller did not develop a password policy for the Town Board (Board) to adopt.

Without effective safeguards, including adequate user account management and written guidance to communicate expectations and current cybersecurity industry standards for configuring and selecting passwords, the risk of a successful cyberattack is significantly increased, particularly given the Town's use of cloud-based services for email communications. Cloud-based systems are directly exposed to the Internet, magnifying the risk of compromise when user account safeguards are inadequate. Cyberattack effects can

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.

2 Service accounts are created for the sole purpose of running a particular network or system service or application. For example, service accounts can be created and used for automatic backups.

include IT system downtime and disruption, the inability to provide services reliant on network and cloud-based resources, data theft (exfiltration) or corruption by malicious actors, and increased remediation and recovery costs.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes five recommendations that, if implemented, will improve the Town's network and cloud-based user account access safeguards from cybersecurity threats. Town officials agreed with our findings and indicated they plan to initiate corrective action.

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 X, Section 5 of the State Constitution. Our methodology and standards are included in Appendix C.

The 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 the New York State 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 Board to make the CAP available for public review in the Town Clerk's office.

Cybersecurity: Findings and Recommendations

Cybersecurity threats are an ever-present organizational risk on par with economic, legal, operational, financial, political and safety risks. Town officials should address cybersecurity risks, as they do any other hazards they encounter, by identifying and mitigating risks, reducing or remediating vulnerabilities and planning for contingencies. This requires an investment of time and resources and a collaborative work environment among the town officials and others responsible to help safeguard network and cloud-based user account access. Many cybersecurity vulnerabilities can be corrected by implementing adequate safeguards at no, or minimal additional cost. It is imperative that town officials partner together to address cybersecurity risks and help protect network and cloud-based user account access from prevalent and emerging cybersecurity threats.

Cybersecurity policies describe the tools and procedures used to help protect IT systems from cybersecurity threats. To safeguard network and cloud-based user account access, town officials should develop policies and written procedures for granting, configuring, safeguarding and managing access, including the importance of using strong passwords.

Town officials should also implement clear procedures for onboarding and offboarding employees to help ensure that user access is granted based on job responsibilities and removed promptly upon employee separation, role changes, extended leave or termination. Disabling accounts in a timely manner is critical to reducing the risk of unauthorized access, especially for former employees or unused accounts. Furthermore, the password policy should establish expectations for configuring and selecting strong passwords and communicate the town's expectations and current cybersecurity industry standards for password security.

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

Finding 1 – The Comptroller did not ensure network user accounts were disabled timely and did not develop a network and cloud user account access policy.

The Comptroller did not ensure all network user accounts were needed and access was adequately managed. We identified 77 enabled user accounts, including 56 employee accounts and 21 service and shared accounts. We determined that 18 employee accounts (32 percent) and four service and shared accounts (19 percent) were unneeded and should have been disabled. The unneeded network user accounts were assigned to former employees who separated from Town employment as early as 2014, for network services no longer actively used, and other accounts referred to by the Comptroller and IT vendor as placeholders and corrupted (meaning there was an error in the accounts' configuration and they may not operate properly).

The Comptroller told us network user accounts were not routinely disabled when employees separated from Town employment because the accounts were used as placeholders until the position vacancy was filled. Also, the IT vendor told us he did not want to disable certain user accounts because he did not know all Town employees and was unaware which user accounts were needed. The IT vendor also told us that while certain user accounts were corrupted and those accounts' users had two enabled network user accounts when they only needed and used one, he needed to keep the corrupted user accounts enabled in case the accounts needed to be accessed.

When network user accounts are unneeded or unused, the accounts should be disabled on the day the employee leaves Town employment or the service or shared account is no longer needed. While unneeded and unused user accounts remain enabled, there is an increased risk of unauthorized access to the Town's network and data. Because the IT vendor was not kept aware of the employment status of Town staff and the Comptroller did not establish procedures to regularly notify the IT vendor of status changes, the IT vendor's ability to disable user accounts in a timely manner was diminished.

The unneeded network user accounts were also not disabled in a timely manner because the Comptroller did not develop a user account access policy for the Board to review and adopt. As a result, network and cloud user account access was not consistently granted, changed and disabled in accordance with defined requirements and current cybersecurity industry standards. Also, network and cloud user account access was not periodically reviewed to help ensure necessity and appropriateness and to identify and disable any unneeded accounts. Without a documented policy and framework for ensuring user account access aligns with Town needs and employees' job duties and responsibilities, Town officials have less assurance that network and cloud user account access is safeguarded from cybersecurity threats.

Although the Comptroller told us she was aware of the importance of a user account access policy, she indicated time constraints hindered her from creating one. In addition, the IT vendor told us he felt a user account access policy was not needed because the Town had a small computing environment. However, a user account access policy has been a longstanding and well-known recommended cybersecurity industry best practice and is beneficial even in smaller environments. Therefore, the Comptroller should have developed a user account access policy for the Board to adopt to help ensure Town expectations and current cybersecurity industry standards were communicated and followed when granting, configuring, safeguarding and managing network and cloud user account access.

Effective network and cloud user account management is key to safeguarding network resources from cybersecurity threats. Unneeded user accounts increase the Town's cyberattack surface because former employees could use the accounts to access sensitive systems, Town records or internal communications, and attackers could attempt to exploit unneeded accounts to launch attacks within the Town's network. As a result, accountability could be undermined due to the reduced ability to reliably attribute account activity to an individual employee.

Furthermore, without clear requirements and standards for network and cloud user account management, former employees may retain user account access, and current employees may have access that is not needed to perform their job duties and responsibilities. These risks are particularly critical in cloud environments, where accessibility extends to the Internet and is more inherently vulnerable to compromise without strong and consistently applied safeguards. Inadequate user account access safeguards also introduce the possibility of noncompliance with regulatory or other requirements, which could result in legal, financial or reputational harm.

Recommendations

The Comptroller should:

1. Develop a comprehensive user account access policy for the Board to adopt to define requirements and standards for granting, configuring, safeguarding and managing network and cloud user account access in accordance with Town expectations and current cybersecurity industry standards.

2. Develop and implement written procedures to periodically review network and cloud user account access for necessity and alignment with Town needs and employees' job duties and responsibilities.

3. Ensure network and cloud user account access is disabled on the day employees leave Town employment and when service and shared accounts are no longer needed.

4. Evaluate all enabled network and cloud user accounts, including employee, shared and service accounts, and disable any that are unneeded in a timely manner.

Finding 2 – The Comptroller did not develop a password policy for the Board to adopt.

The Comptroller did not utilize the IT Vendor to develop a password policy for the Board to adopt that defined and communicated the Town's expectations and current cybersecurity industry standards for passwords used to access network and cloud user accounts. As a result, Town employees and the IT vendor did not have documented requirements or guidance for configuring and selecting passwords, such as password length and complexity, comparisons and changes, invalid password attempt thresholds, encryption or other requirements necessary to help safeguard accounts from cybersecurity threats. Consequently, Town officials have less assurance that passwords are managed and used in a consistent or secure manner across the Town's network and cloud environments, which could increase the risk of critical user accounts and sensitive data being compromised. The increased risk is further compounded by the unneeded accounts discussed in Finding 1.

Although the Comptroller told us she was aware of the importance of a password policy, she indicated time constraints hindered her from creating one. In addition, the IT vendor told us he felt a password policy was not needed because the Town had a small computing environment. However, a password policy has been a longstanding and well-known recommended cybersecurity industry best practice and is beneficial even in smaller environments. Therefore, the Comptroller should have developed a password policy for the Board to adopt to help ensure Town expectations and current cybersecurity industry standards were followed when configuring, selecting, safeguarding, reviewing and managing network and cloud user account passwords.

Without clear requirements and standards for network and cloud user account passwords, weak passwords may be allowed and used to access the Town's network and cloud resources, substantially increasing the likelihood of unauthorized access. The risks are magnified in cloud environments where user accounts may be directly accessible from the Internet and serve as entry points to critical services, such as email communications and confidential information. Without strong password requirements and guidance, the risk of data breaches, service disruptions and loss of public trust is further heightened. In addition, inadequate network and cloud user account password practices could introduce the possibility of noncompliance with regulatory, contractual or other requirements, which could result in legal, financial or reputational harm.

Recommendation

5. The Comptroller should develop a comprehensive password policy for the Board to adopt to define requirements and standards for configuring, selecting, safeguarding, reviewing and managing network and cloud user account passwords.

Appendix A: Profile, Criteria and Resources

Profile

The Town, located in Saratoga County, is governed by the elected Board composed of the Town Supervisor and four Councilmembers and serves 17,361 residents. The Board is responsible for overseeing the Town's operations and financial activities.

The Town uses a third-party IT vendor to help oversee the Town's IT environment. The Comptroller is responsible for the Town's website, and ensuring the services provided by the IT vendor are performed adequately in accordance with the vendor contract. The Comptroller, along with the IT vendor, is responsible for establishing controls over network and cloud-based user account access.

Town officials and employees use Town-owned IT assets (e.g., computers, laptops and tablets) to perform day-to-day operations and access stored information collected by the Town. The Town relies on its network and cloud-based user accounts to access these IT assets for Internet access, email and maintaining various records, such as financial and personnel records, engineering documents, public safety information and other information that may contain PPSI.

Criteria

Officials should establish procedures to actively manage user accounts to ensure that access is limited only to individuals who require access for official duties. Accounts assigned to former personnel and for IT services, such as service and shared accounts, should be disabled on the day users separate from Town employment or the accounts are no longer needed. Disabling user accounts in a timely manner is important to prevent inappropriate access by unauthorized individuals. A periodic review process will help to ensure that all user accounts remain appropriate and necessary.

To strengthen a town's cybersecurity posture, officials should develop a comprehensive network and cloud user account access policy for the town board to adopt, and written procedures to help ensure policy compliance. The policy and procedures should clearly define how user accounts are created, modified, reviewed and disabled, and document user roles and access levels. Regular account reviews help ensure that all user accounts remain necessary and consistent with employees' current job duties and responsibilities. Documentation also provides accountability and a record of approvals, reducing the risk of inappropriate or unauthorized access to the town's network.

To help safeguard the town's network and cloud user account access, officials should develop a comprehensive password policy for the town board to adopt. A password policy establishes rules for the creation, use and management of network and cloud user account passwords. The password policy should establish expectations for IT administrators configuring password settings and for users selecting passwords. The password policy should communicate current industry standards for password security. At a minimum, the policy should define any requirements for password length and complexity, comparison and changes, invalid password attempt thresholds, encryption or other requirements necessary to help safeguard accounts from cybersecurity threats, such as secure procedures for resetting forgotten passwords and standards that prohibit password sharing. Officials should periodically review and update the password policy to ensure it reflects evolving cybersecurity industry standards.

Cybersecurity policies should be communicated to all network and cloud users and include procedures to ensure compliance. This helps reduce the risk of data, hardware and software being lost, damaged or compromised by unauthorized access and misuse.

Additional Resources

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

- *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

- *Information Technology Governance*: https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf

In addition, local officials can use our 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 and 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 WILTON
22 Traver Road
Gansevoort, New York 12831-9127
(518) 587-1939
FAX (518) 5877
www.townofwilton.com
Dr. Toni Sturm, Town Supervisor

July 30, 2026

Jennifer Kenneson
Chief Information Systems Auditor
110 State Street
Albany, NY 12236

Dear Ms. Kenneson,

The Town of Wilton is in receipt of the Office of the State Comptroller's Cybersecurity draft audit report, 2026M-48, which covers the period January 1, 2024 – August 8, 2025. The Town is respectfully responding to the report.

The Town agrees with the findings included in the report and appreciates the recommendations provided by the Office of the State Comptroller, as these will enhance our procedures to ensure a strong network environment. The User Access and Password policies referenced in the Town's responses below are the result of the recommendations provided by OSC.

OSC Recommendation Number 1:
Develop a comprehensive user account access policy for the Board to adopt to define requirements and standards for granting, configuring, safeguarding and managing network and cloud user account access in accordance with Town expectations and current cybersecurity industry standards.

Town of Wilton Response:
The Town Board has adopted a User Access Policy which prescribes procedures for granting, changing and revoking access to the network and establishes who has the authority to grant or change access.

OSC Recommendation Number 2:
Develop and implement written procedures to periodically review network and cloud user account access for necessity and alignment with Town needs and employees' job duties and responsibilities.

Town of Wilton Response:
The User Access Policy states that users are only given access to applications necessary to perform their job duties. Procedures to periodically review network and cloud user account access will be incorporated into the User Access Policy.

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

OSC Recommendation Number 3:
Ensure network and cloud user account access is disabled on the day employees leave Town employment and when service and shared accounts are no longer needed.

Town of Wilton Response:
The User Access Policy includes procedures and documentation for disabling user access upon termination.

OSC Recommendation Number 4:
Evaluate all enabled network and cloud user accounts, including employee, shared and service accounts, and disable any that are unneeded in a timely manner.

Town of Wilton Response:
The User Access Policy includes procedures for the review of user accounts. Dormant accounts have been deleted. Going forward, all user accounts will be evaluated regularly to ensure that they are needed.

OSC Recommendation Number 5:
Develop a comprehensive password policy for the Board to adopt to define requirements and standards for configuring, selecting, safeguarding, reviewing and managing networks and cloud user account passwords.

Town of Wilton Response:
The Town Board has adopted a Password Policy to define password length, complexity, expiration, disguise, reset and lockout.

Sincerely,

Dr. Toni Sturm, Town of Wilton Supervisor

Appendix C: Audit Methodology and Standards

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

- We communicated with Board members regarding network and cloud-based user account cybersecurity threats and safeguards. We reviewed the Town's cybersecurity policies and procedures and interviewed the Comptroller and IT vendor to gain an understanding of network and cloud-based user account access and safeguards.

- We ran computerized audit scripts on the Town's network on June 24 and July 22, 2025, and observed the Town's cloud computing environment on August 7, 2025. We identified all enabled 77 network and 110 cloud user accounts and reviewed and compared the security settings for all enabled network and cloud user accounts to current cybersecurity industry standards to identify any inconsistencies.

- We obtained a list of all active Town employees from the Comptroller to match enabled network and cloud user accounts to active employees.

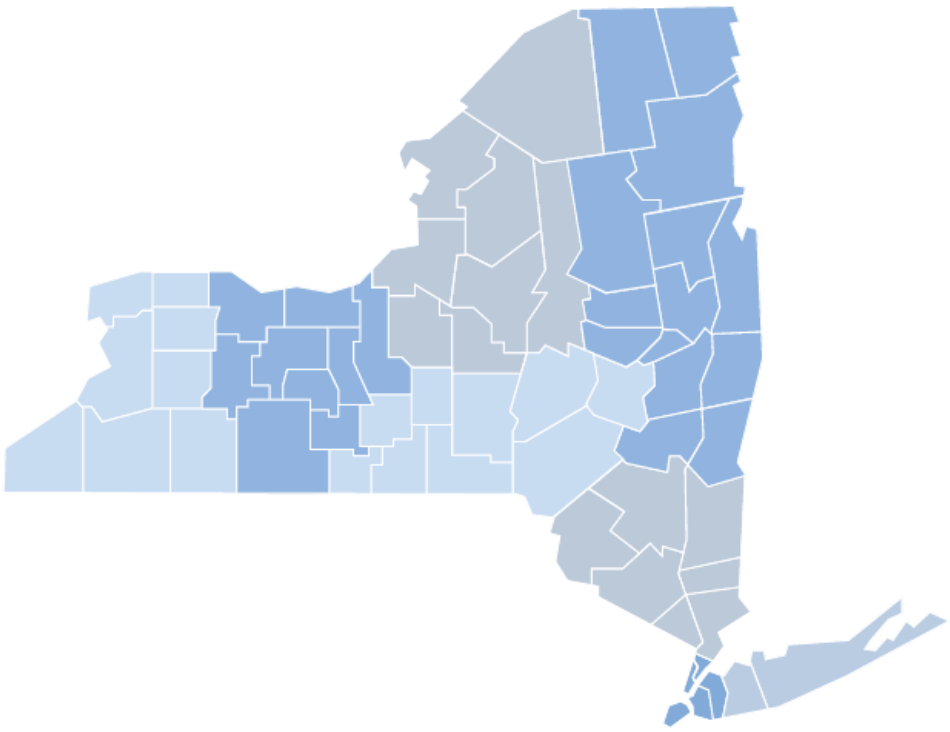
- We interviewed the Comptroller and IT vendor to obtain explanations for network and cloud user accounts with potentially unneeded permissions and to discuss user accounts that did not match an active Town employee on the list provided.

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 Town officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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.

Questions?

APPLIED TECHNOLOGY UNIT
Jennifer Kenneson, Chief Information Systems Auditor
110 State Street, 12th Floor • Albany, New York 12236
Tel (518) 738-2639 • Fax (518) 486-6479
Email: Muni-Cyber@osc.ny.gov



Contact

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

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability

FOLLOW US: osc.ny.gov/subscribe