DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-77

Town of Pelham

Information Technology

AUGUST 2019

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

Contents

Report Highlights

Town of Pelham

Audit Objective

Determine whether the Town Board ensured the Town's IT systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

- Personal Internet use was found on computers assigned to 10 employees who routinely accessed personal, private and sensitive information.
- Town officials did not provide IT security awareness training for individuals who used Town IT assets.
- Town Board and officials did not develop comprehensive IT policies or procedures.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Provide adequate oversight of employee Internet use to ensure it complies with Board policies.
- Provide employees with annual IT security awareness training.
- Adopt comprehensive IT policies that address acceptable use, IT security awareness training, breach notification and disaster recovery planning and communicate all IT policies to officials, employees and the IT consultant.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Town of Pelham (Town) is located in Westchester County. The Town is governed by an elected Town Board (Board) that includes a Supervisor and a four-member Town Council.

The Board is responsible for providing oversight of the Town's operations. The Supervisor is the Town's chief financial officer and chief executive officer and is responsible, along with other administrative staff, for the Town's day-to-day administration.

The Town contracted with an IT consultant who reviewed and updated the Town's computer systems to ensure system and hardware versions were current. He also performed problem solving on an on-call basis.

Quick Facts	
Number of Employees	103
IT Users	15
Network Accounts	15
Number of Computers	15

Audit Period

January 1, 2017 – November 13, 2018. We extended our scope forward to December 20, 2018 to complete computer testing.

Information Technology Governance

The Town relies on its information technology (IT) system to perform a variety of tasks, including providing Internet access, protecting personal, private and sensitive information (PPSI),[1] email communication, recording financial transactions and reporting to State and federal agencies and for maintaining financial and personnel records.

The Town's Comptroller and bookkeeper served as administrators of the Town's financial software.

How Does an Acceptable Use Policy Secure and Protect the Town's IT Systems?

An acceptable use policy (AUP) describes what constitutes appropriate and inappropriate use of IT resources, along with the Board's expectations concerning personal use of IT equipment and user privacy.[2] Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, AUPs or standard security practices. Automated mechanisms may be used to perform this process and can help security professionals routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access. According to the Town's employee handbook, Town-owned computers and email accounts are to be used for appropriate business purposes only.

Some Town Computers Were Used For Personal Activities

The Town did not have an AUP. We reviewed the technology use section of the employee handbook and found that it did not clearly define use that was not acceptable or the consequences of violating the computer and communication systems.

We reviewed the web browsing history for 10 computers[3] used by 10 employees and found significant personal Internet use on all 10 computers that was not related to Town-business. This included social media use and accessing entertainment and leisure websites.[4]

[1] Personal, private and sensitive information (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] For example, management may reserve the right to examine email, personal file directories, web access and other information stored on computers, at any time and without notice.

[3] Refer to Appendix B for further information on our sample selection.

[4] Including Netflix, YouTube, Pandora (a music service) and online consumer magazines such as People and US Weekly

All 10 employees' job duties included routinely accessing PPSI. As a result, their personal Internet use unnecessarily exposed this information to being compromised.

Town officials were unaware of this personal computer use because they did not routinely monitor employee Internet use or have procedures designed to monitor IT usage and enforce compliance with the technology use section of the employee handbook. Also, the Town's IT consultant was unable to enforce the Town's technology use policy because he was not aware of its existence.

Inappropriate or questionable use of Town computers could expose the Town to malicious software infections that compromise systems and data, including PPSI. Also, when employees access websites for nonbusiness or inappropriate purposes through the Town's network, productivity is reduced.

Why Should Town Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, Town officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees. The training should center on emerging trends such as information theft, social engineering attacks[5] and computer viruses and other types of malicious software, all of which may result in PPSI compromise or expose the Town to ransomware attacks. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that 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; any requirements related to protecting PPSI; the risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

IT Users Were Not Provided With IT Security Awareness Training

Town officials did not develop adequate policies and procedures to ensure that Town employees receive proper IT security awareness training to protect IT assets. Also, during our audit period, Town officials did not provide users with IT security awareness training to help ensure they understood IT security measures.

[5] Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. Town officials cannot protect 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 IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise the Town's IT assets and security. As a result, data and PPSI are at a greater risk for unauthorized access, misuse or loss.

Why Should the Town Manage User Accounts and Access?

Network user accounts are potential entry points for attackers because they could be used to inappropriately access and view PPSI in a financial system. A town should have a written policy and procedures for granting, changing and revoking access rights to the network and to specific software applications.

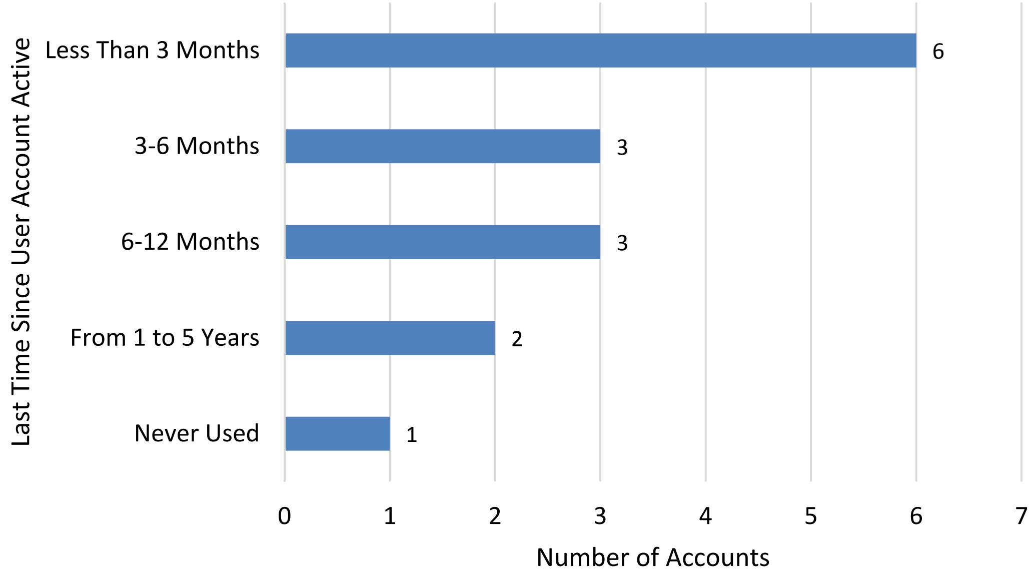
In addition, to minimize the risk of unauthorized access, town officials should regularly review enabled network user accounts to ensure they are still needed. Officials must disable unneeded accounts as soon as there is no longer a need for them, including user accounts of former employees or employees who have transferred to another area. The IT consultant is responsible to ensure user accounts for the IT system are managed in a timely and satisfactory manner.

Officials Did Not Adequately Manage Inactive User Accounts

Town officials did not develop comprehensive written procedures for managing system access. During our review of all 15 network accounts, we found that five (33 percent) had not been used in six months or more (Figure 1).

FIGURE 1

User Account Login Activity



The IT consultant was unaware that these accounts were inactive. Because the Town did not have formal procedures for regularly reviewing enabled user accounts, the inactive user accounts went unnoticed until our audit. In addition, because they were not monitored, the Town had a greater risk that the IT consultant would not have noticed if the accounts had been compromised or used for malicious purposes.

In addition, we found that two accounts (13 percent) did not match the employee master list. Both accounts belonged to former Town employees and should have been disabled immediately after the employees left Town employment.

Officials told us they notified their IT vendor by email when employees left Town employment but were unaware that these accounts were not disabled. User accounts of former employees that have not been disabled or removed could potentially be used by those individuals or others for malicious purposes.

Why Should the Town Have a Breach Notification Policy?

The New York State Technology Law[6] requires municipalities and other local agencies to have a breach notification policy or local law that requires notification be given to certain individuals in the event of a system security breach, as it relates to private information. The policy should detail how officials would notify

[6] New York State Technology Law Section 208

individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization.

The disclosure should be made in the most expedient time possible consistent with legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Private information includes social security numbers, bank account numbers, healthcare information, credit and debit card numbers and driver's license information.

The Board Did Not Adopt a Breach Notification Policy

The Board did not adopt an information breach notification policy. The Comptroller told us that the Town did not adopt a breach notification policy or local law because it was unaware of the legal requirement to do so. Without a formal breach notification policy, the Town may not be able to fulfill its legal obligation to notify affected individuals if sensitive information is compromised.

Why Should the Town Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, Town officials should establish a formal written disaster recovery plan (plan). This is particularly important given the current and growing threat of ransomware attacks. The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the financial system and any PPSI contained therein. Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations.

The Board and Town Officials Have Not Established a Disaster Recovery Plan

The Board did not adopt a comprehensive written plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster, Town personnel have no guidance or plan to follow to restore or resume essential operations in a timely manner. Without a formal, written plan, the Town has an increased risk that it could lose important data and suffer serious interruption in operations, such as not being able to process checks to pay vendors or employees.

What Should Be Included in an IT Vendor Contract?

A written contract provides both parties with a clear understanding of the services expected to be provided and a legal basis for compensation provided for those services. The Board should have a formal written contract with its IT provider that specifies the contract period, services to be provided and basis of compensation for those services.

In addition, to protect the Town and avoid potential misunderstandings, officials should have a written service level agreement (SLA) between the Town and its IT consultant that identifies the Town's needs and expectations and specifies the level of service to be provided by the IT consultant.

An SLA is different from a traditional written contract in that it establishes comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement; scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The Town Did Not Have a Written Contract or Service Level Agreement With its IT Consultant

Although the Town paid its IT consultant $13,635 in 2017 and $10,414 in 2018, officials were unable to provide us with a copy of the Town's contract with its IT consultant. Town officials told us they called the IT consultant whenever they had questions or needed assistance.

Without a formal contract, Town officials did not have a documented understanding of the level of compensation to be paid to the IT consultant or services expected to be provided by the vendor. Also, the Town did not have contractual or legal protection if the IT consultant defaulted on his obligations.

The Town also did not have a written SLA with its IT consultant to define service level objectives; performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval processes; and payment and scope of services to be provided.

Without a written SLA, the IT consultant did not have accountability for various aspects of the Town's IT environment. As a result, the Town had a greater risk that its computer resources and PPSI could have been accessed by attackers, misused or abused.

What Do We Recommend?

The Board should:

1. Adopt an acceptable use policy, IT security awareness training policy, breach notification policy and disaster recovery plan and communicate all adopted IT policies and the plan to officials, employees and the IT consultant.
2. Enter into a formal written contract with the Town's IT consultant.
3. Develop an SLA with the Town's IT consultant to address the Town's specific needs and expectations for IT services.

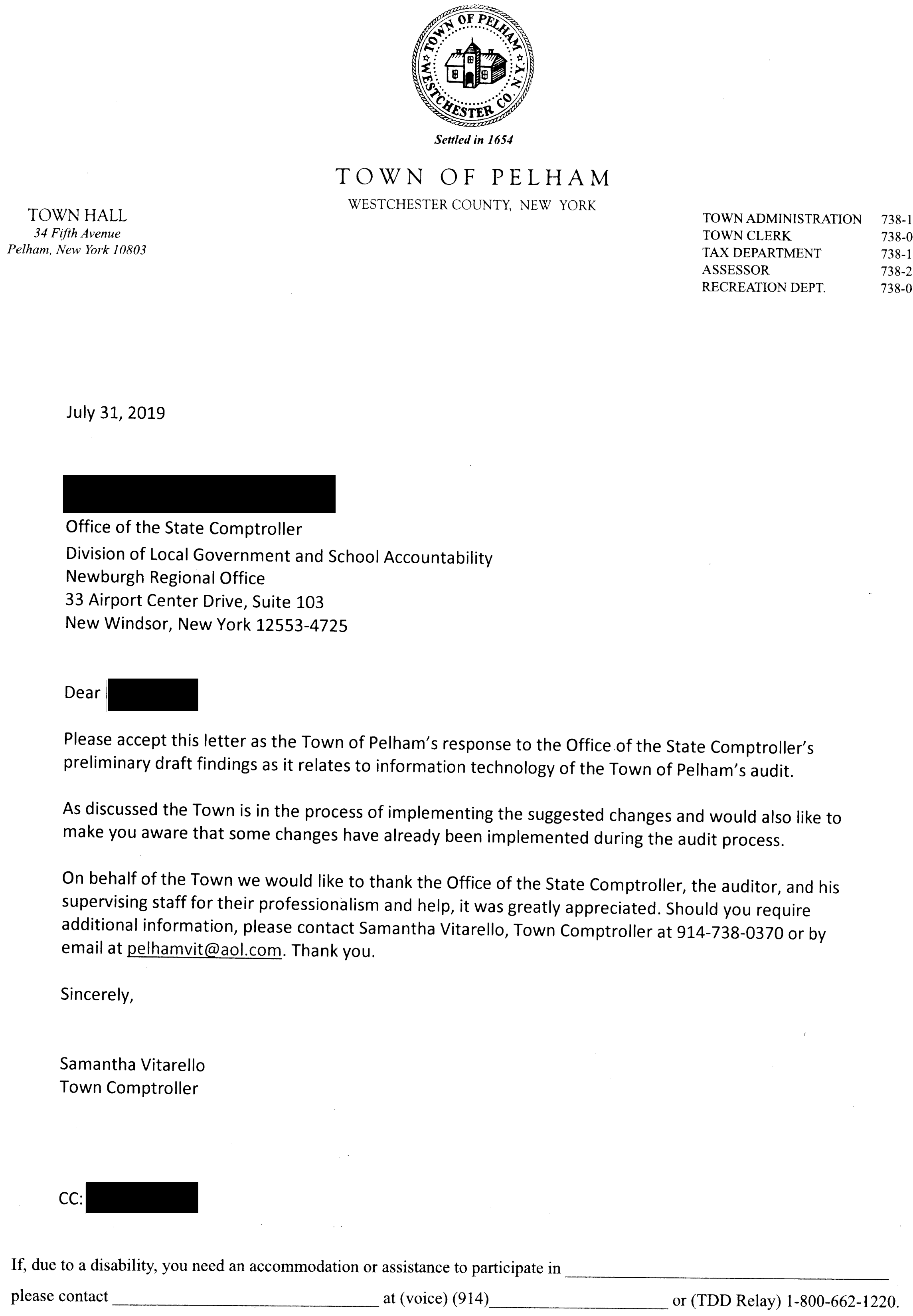
Town officials should:

4. Develop comprehensive written procedures for IT security awareness training, managing system access and regularly reviewing enabled user accounts.
5. Provide IT users with IT security awareness training at least annually.

Town officials should ensure the IT consultant:

6. Monitors employee Internet usage and enforces the Town's technology use policy.
7. Regularly reviews enabled user accounts and immediately disables user accounts when access is no longer needed.

Appendix A: Response From Town Officials



Settled in 1654

TOWN OF PELHAM
WESTCHESTER COUNTY, NEW YORK

TOWN HALL
34 Fifth Avenue
Pelham, New York 10803

TOWN ADMINISTRATION	738-1021
TOWN CLERK	738-0777
TAX DEPARTMENT	738-1642
ASSESSOR	738-2878
RECREATION DEPT.	738-0153

July 31, 2019

[redacted]
Office of the State Comptroller
Division of Local Government and School Accountability
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Dear [redacted]

Please accept this letter as the Town of Pelham's response to the Office of the State Comptroller's preliminary draft findings as it relates to information technology of the Town of Pelham's audit.

As discussed the Town is in the process of implementing the suggested changes and would also like to make you aware that some changes have already been implemented during the audit process.

On behalf of the Town we would like to thank the Office of the State Comptroller, the auditor, and his supervising staff for their professionalism and help, it was greatly appreciated. Should you require additional information, please contact Samantha Vitarello, Town Comptroller at 914-738-0370 or by email at pelhamvit@aol.com. Thank you.

Sincerely,

Samantha Vitarello
Town Comptroller

CC: [redacted]

If, due to a disability, you need an accommodation or assistance to participate in ______________________
please contact ______________________ at (voice) (914)______________ or (TDD Relay) 1-800-662-1220.

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, we performed the following audit procedures:

- We reviewed the Town's policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed officials and personnel to gain an understanding of internal controls over IT and online banking.
- We ran a specialized audit script on the Town's and recreation department's domain controllers.[7] We then analyzed the reports to identify inactive user accounts.
- We used our professional judgment to select a sample of 10 computers with 10 users. The 10 computers included five located in the Finance department and five in the Recreation department. The 10 users included five Finance department employees who had access to key financial applications and related PPSI, including online banking, payroll and human resources data. Their titles included the Town Comptroller, Town Clerk, bookkeeper, assessor and deputy receiver of taxes. The remaining five employees worked in the Recreation department and had job duties and IT user privileges that involved using and transmitting important electronic financial data. Their titles included three recreation leaders, one senior advocate and one recreation supervisor. We reviewed web history reports on the 10 selected computers to identify names of websites accessed that could put the network at risk.
- We inquired about a disaster recovery plan.
- We reviewed the level of services provided by the IT consultant and inquired to determine whether the Town had a formal written contract with the provider.
- We reviewed user access to the online banking application and evaluated user permissions to determine whether there was a proper segregation of duties and whether granted access was necessary for users to perform their assigned duties.

Our audit also examined the adequacy of certain information technology 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.

[7] The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

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.

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 size of the relevant population and the sample selected for examination.

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 Board to make the CAP available for public review in the Town Clerk’s office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/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/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

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

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/localgov/index.htm

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

NEWBURGH REGIONAL OFFICE

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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