DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-28

Town of Pulteney

Information Technology

JUNE 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Town of Pulteney

Audit Objective

Determine whether Town of Pulteney (Town) officials adequately safeguarded Town information technology (IT) assets.

Key Findings

Town officials did not adequately safeguard Town IT assets and failed to implement the recommendations we made in 2013 to adopt comprehensive IT security policies and monitor computer use. As a result, we found officials did not:

- Adopt key IT policies or a comprehensive IT contingency plan to minimize the risk of data loss or suffering a serious interruption of services.
- Monitor the use of IT resources or provide IT security awareness training.
- Disable four unneeded local user accounts.
- Enter into a service level agreement (SLA) with the Town's IT service providers.

In addition, sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT security policies and a comprehensive IT contingency plan.
- Regularly review user accounts and disable those that are unnecessary.
- Enter into an SLA with the IT service providers for all services to be provided.

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

Background

The Town, located in the northeast corner of Steuben County, is governed by an elected Town Board (Board), composed of a Supervisor and four Board members. The Board is responsible for the general oversight of operations and finances, including establishing policies and procedures to safeguard IT assets and provide a secure IT environment.

Town employees and officials use the Town's IT assets to initiate, process, record and report transactions and rely on the IT systems for Internet access and email. The Town's IT service provider is an unpaid volunteer, who services Town computers on an as needed basis.

During our previous audit of the Town, we identified IT security weaknesses. Refer to *Town of Pulteney – Financial Management and Information Technology (2012M-177)*, issued in April 2013.

Quick Facts	
Employees	20
Computers	6
Local User Accounts	13

Audit Period

January 1, 2019 – February 23, 2021

Information Technology

What Policies and Procedures Should the Board Adopt To Safeguard IT Assets and Data?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential that a board establish security policies for key IT security issues, such as those related to user accounts and permissions, security awareness, data breach and classification and business continuity.

As it develops such policies, a board should take into account people, processes and technology. Further, a board should periodically review these policies, update them as needed, designate personnel who are responsible for monitoring policy compliance and communicate the policies to all users.

It is important that a board adopt an acceptable computer use policy (AUP) that defines procedures for acceptable computer, Internet and email use and specific consequences for violations. Officials can reduce the risks to personal, private and sensitive information (PPSI),[1] and IT assets by monitoring Internet use and developing and implementing procedures to ensure employees comply with the AUP.

...[I]t is essential that a board establish security policies for... user accounts and permissions, security awareness, data breach and classification and business continuity.

The Board Failed to Adopt any IT Policies or Provide IT Security Awareness Training

During our audit period, the Board did not adopt any IT policies and procedures, including those addressing key IT security issues, such as user accounts and permissions, security awareness, breach notification and data classification, business continuity or acceptable computer use. In addition, the Board did not provide IT security awareness training to employees using Town computers.

During our previous audit of the Town, we identified similar findings and stressed the importance of developing and implementing IT policies and procedures and monitoring computer use. Refer to *Town of Pulteney – Financial Management and Information Technology (2012M-177)*, issued in April 2013. However, over the last seven years, the Board did not develop any IT security policies, such as an AUP or breach notification.

Because the Board did not adopt an AUP governing appropriate use of IT assets, monitor employee Internet use for inappropriate or unusual activity and provide employees with IT security awareness training, we reviewed the Internet browsing histories of all six computers.

During our previous audit... we identified similar findings and stressed the importance of developing... IT policies... and monitoring computer use... [and] over the last seven years, the Board did not develop any IT security policies...

[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 found two computers showed the user accessed a large percentage (43 to 51 percent) of advertising websites when compared to the total number of websites visited. Large percentages of these types of websites, which present unwanted advertisements to computer users, could indicate malicious software. Because three of the six computers lacked antivirus software, there was an increased risk that malicious software could be installed and undetected. Further, we found one computer was used for personal use, such as accessing a social media website.

While comprehensive policies will not guarantee the safety of IT assets and data, the failure to adopt policies and provide IT security awareness training significantly increases the risk that users will not understand their responsibilities, putting the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse. Further, without a breach notification policy, the Town may not be able to fulfill its legal obligation to notify affected individuals that they should monitor their credit reports and bank activity because their sensitive and private information was compromised.

...[O]ne computer was used for personal use, such as accessing a social media website.

Why Should the Board Adopt an IT Contingency Plan?

An IT contingency plan is a town's recovery strategy, composed of the procedures and technical measures that enable the recovery of IT operations after an unexpected incident. An unexpected incident could include a power outage, software failure caused by a virus or malicious software, equipment destruction, or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such an event.

The content of, length of and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the town's computer operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

Because IT often supports key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining an organization's critical business processes in the event of a disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Policies and procedures are also critical components and ensure that information is routinely backed up and available in the event of a disruption.

The IT contingency plan can also include, among other items deemed necessary by the organization, the following:

- Roles and responsibilities of key personnel
- Periodic training regarding the key personnel's responsibilities
- Communication protocols with outside parties
- Prioritized mission critical processes
- Technical details concerning how systems and data will be restored
- Resource requirements necessary to implement the plan
- Backup methods and storage policies
- Details concerning how the plan will be periodically tested.

The Board Did Not Adopt an IT Contingency Plan

The Board did not develop a comprehensive IT contingency plan to describe the measures officials would take to respond to potential disruptions and disasters affecting IT. Consequently, in the event of a disruption, a disaster, phishing[2] or a ransomware attack, employees have no guidance to follow to restore or resume essential operations in a timely manner.

The Board did not develop a comprehensive IT contingency plan to describe the measures officials would take to respond to potential... disasters affecting IT.

Without a comprehensive plan, there is an increased risk that the Town could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Although Town officials told us that the financial data was backed up regularly, no backups were stored offsite, and the backups were not tested periodically to ensure they functioned as expected.

Although officials hired an IT service provider after our prior 2013 audit to implement some of our recommendations, this individual no longer served the Town during our audit period. Other than using the services of an unpaid volunteer, who serviced Town computers on an as needed basis, the Board did not take any measures to implement corrective action after the former IT service provider's departure.

Having the backup data stored in the same location as the original data puts the data at risk for total loss if there is a catastrophic event. Without periodic testing of backups, the Board cannot ensure the recovery of necessary data to continue operations if a security breach or system malfunction occurs. Without a viable

[2] Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.

plan, the Town is at risk of significant disruptions in business operations after a disastrous event and could suffer unnecessary and preventable losses.

Why Should Officials Manage User Accounts and Permissions?

Town officials are responsible for restricting user access to only those applications, resources and data needed to complete job duties and responsibilities. This helps ensure data and IT assets are protected from unauthorized use and/or modification.

Local user accounts enable computers and applications to recognize specific users, grant appropriate permissions and provide user accountability by affiliating user accounts with specific users. These accounts are potential entry points for attackers because, if compromised, they could be used to access and view data stored on the computer.

To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner. The Board should adopt written procedures for granting, changing and disabling user access to the computers.

Generally, administrative accounts have oversight and control of computers and applications, with the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, any program that a user with local administrative permissions runs will inherently run with the same permissions. For example, if malicious software installed itself on a computer, it would run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of computer compromise and/or data loss. Officials must limit administrative permissions to those users who need them to complete their job functions.

Officials Did Not Adequately Manage User Accounts and Permissions

Officials did not adequately manage user accounts and permissions because the IT service provider was an unpaid volunteer who was unaware of the need to properly manage them. As a result, the Town had unneeded and unused local user accounts that had not been disabled and/or monitored.

Our review of the Town's six computers identified 13 local user accounts. We found three local user accounts (23 percent) were not used in at least four years,

We found three local user accounts (23 percent) were not used in at least four years, one of which was never used.

one of which was never used. Further, while 12 of 13 local user accounts had administrative permissions, only six accounts needed these permissions.

When unnecessary user accounts are not removed in a timely manner and users have unneeded administrative permissions, the risk of unauthorized access and changes that might not be detected is increased. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

A user can be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website, or accessing a website programmed to automatically infect the user's computer with malicious software. If the deceived user has administrative permissions, an attacker could use those elevated privileges to cause greater damage than with a lesser-privileged account.

Why Should the Board Have an SLA With its IT Service Provider?

The Board must ensure that it has qualified IT personnel to manage the Town's IT environment. This can be accomplished by using Town employees, an IT service provider or both. To protect Town assets and avoid potential misunderstandings, the Board should have a written SLA with the Town's IT service provider that clearly identifies the Town's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI.

An SLA is different from a traditional written contract in that it establishes comprehensive, measurable 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 processes; and pricing, billing and terms of payment.

The SLA should be periodically reviewed, especially if the IT environment or needs change significantly.

The Board Did Not Have an SLA with its IT Service Providers

The Board did not have an SLA or written contract with the IT service provider because the IT service provider was an unpaid volunteer who entered into a verbal agreement with Town officials to fix computers, install new hardware and software, and make recommendations for purchases, on an as needed basis. Further, because the Board's composition changed over the past eight years and current Board members had five years or less of governing experience, it chose to accept the risk associated with not formalizing its agreement. Also, the Board had another IT service provider for the water department, but officials did not provide us with any details about this provider.

Without a written SLA, the Board and IT service providers do not have stated responsibilities and procedures for how to resolve any failures in IT controls, service disruption or data breach. This can contribute to confusion over who has responsibility for the various aspects of the Town's IT environment, which could put the Town's computer resources and data at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies to address user accounts and permissions, security awareness, breach notification and data classification and business continuity.

2. Adopt an AUP to clearly define what an acceptable level of personal use is, and identify penalties for violation of this policy.

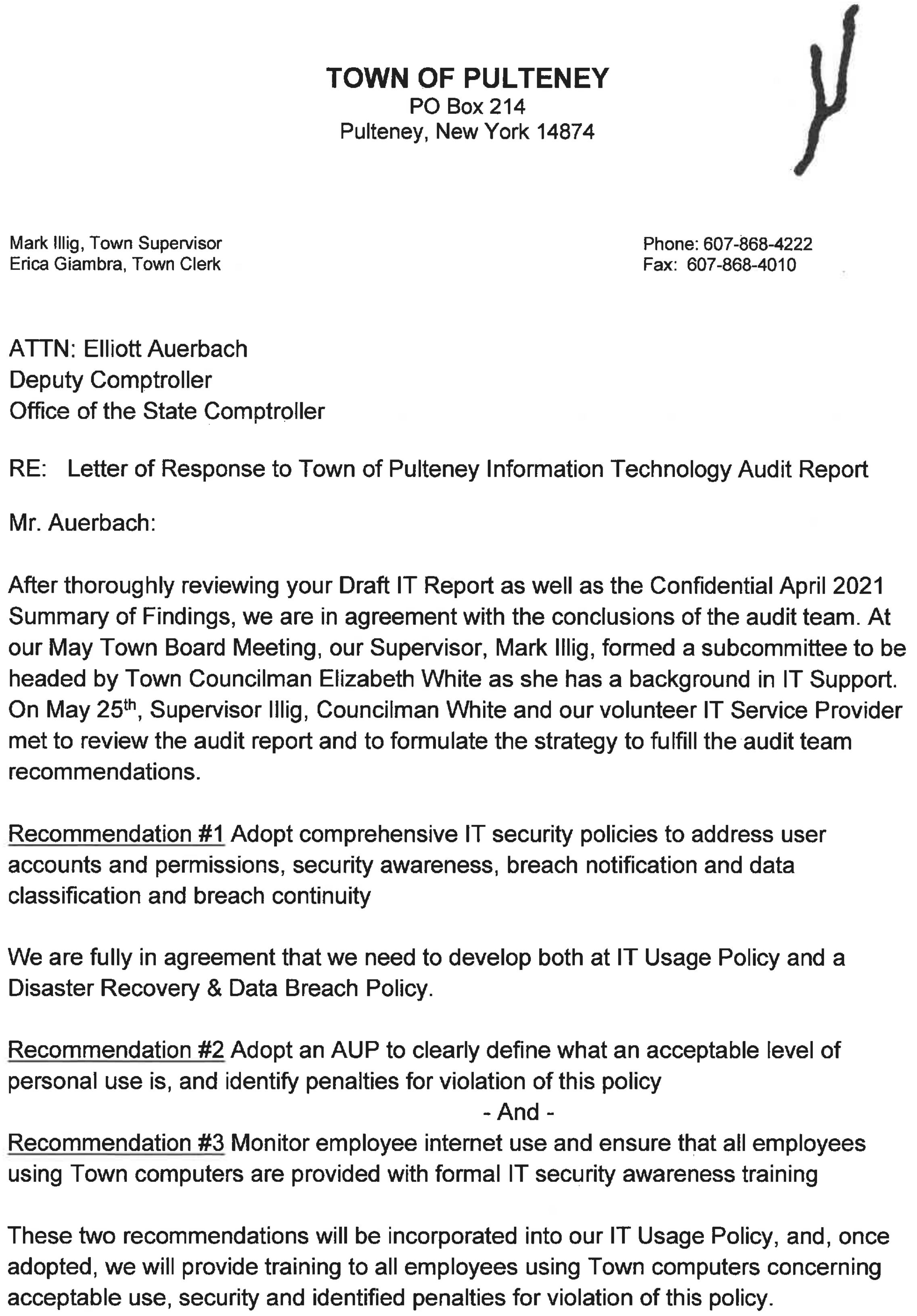
3. Monitor employee Internet use and ensure that all employees using Town computers are provided with formal IT security awareness training.

4. Develop and adopt a comprehensive disaster recovery plan, including data backup procedures and off-site storage.

5. Have someone assess user accounts and permissions on a regular basis and remove or disable unnecessary accounts.

6. Develop an SLA with the IT service providers to address the Town's specific needs and expectations for IT services and the roles and responsibilities of all parties.

Appendix A: Response From Town Officials



TOWN OF PULTENEY
PO Box 214
Pulteney, New York 14874

Mark Illig, Town Supervisor
Erica Giambra, Town Clerk

Phone: 607-868-4222
Fax: 607-868-4010

ATTN: Elliott Auerbach
Deputy Comptroller
Office of the State Comptroller

RE: Letter of Response to Town of Pulteney Information Technology Audit Report

Mr. Auerbach:

After thoroughly reviewing your Draft IT Report as well as the Confidential April 2021 Summary of Findings, we are in agreement with the conclusions of the audit team. At our May Town Board Meeting, our Supervisor, Mark Illig, formed a subcommittee to be headed by Town Councilman Elizabeth White as she has a background in IT Support. On May 25th, Supervisor Illig, Councilman White and our volunteer IT Service Provider met to review the audit report and to formulate the strategy to fulfill the audit team recommendations.

Recommendation #1 Adopt comprehensive IT security policies to address user accounts and permissions, security awareness, breach notification and data classification and breach continuity

We are fully in agreement that we need to develop both at IT Usage Policy and a Disaster Recovery & Data Breach Policy.

Recommendation #2 Adopt an AUP to clearly define what an acceptable level of personal use is, and identify penalties for violation of this policy

- And -

Recommendation #3 Monitor employee internet use and ensure that all employees using Town computers are provided with formal IT security awareness training

These two recommendations will be incorporated into our IT Usage Policy, and, once adopted, we will provide training to all employees using Town computers concerning acceptable use, security and identified penalties for violation of this policy.

Recommendation #4 Develop and adopt a comprehensive disaster recovery plan, including data backup procedures and offsite storage.

As the Town's six computers are single user machines dedicated to a task and user with no network server, we plan to utilize available software to handle backups on a regular, consistent and more automated basis, and we will be reviewing the pros and cons of utilizing the cloud versus system imaging and thumb drive backups stored onsite in a fireproof safe or a combination of the two.

Following the audit, we have replaced three computers (Clerk, Bookkeeper and Water Department) eliminating the issues of older, out-of-date software and allowing for system updates for software and automated security patches. Our Assessor's computer and Lauren's PC have been scheduled for replacement as well.

Recommendation #5 Have someone assess user accounts and permissions on a regular basis and remove or disable unnecessary accounts

This will be addressed as part of the IT Usage Policy defining users, permissions and unnecessary accounts. Once we have the policy, we will identify who will be responsible.

Recommendation #6 Develop an SLA with the IT service providers to address the Town's specific needs and expectations for IT services and the roles and responsibilities of all parties.

We are in agreement that we need to formalize Service Level Agreements with our IT service providers.

In conclusion, we are in agreement with your IT findings and have begun the processes necessary for drafting an IT Usage Policy and a Disaster Recovery Policy and Plan and are reviewing service provider relationships and the necessary SLAs.

Respectfully submitted,

Elizabeth White
Pulteney Town Councilman and IT Subcommittee Lead

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[3] and obtain valid audit evidence, our audit procedures included the following:

- We interviewed officials and the IT service provider to gain an understanding of IT operations.
- We ran a web history computerized audit script on six Town computers and then reviewed the Internet use and web history to evaluate whether Internet use was appropriate and if unnecessary exposure of PPSI had occurred.
- We ran a configurations computerized audit script on six computers. We then analyzed the results generated by the scripts to obtain information about the computers' users to determine whether user account and security settings were necessary and appropriate. We reviewed user accounts to identify potentially inactive and unnecessary accounts. We also analyzed user accounts and security settings applied to those accounts.
- We followed up with officials and the IT service provider to determine whether there were any unneeded accounts and any automated settings that indicated ineffective IT controls.

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.

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.

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 General Municipal Law. For more information on preparing and filing your

[3] We also issued a separate audit report, *Town of Pulteney – Financial Condition (2021M-24).*

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
https://www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://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
https://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
https://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
https://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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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