REPORT OF EXAMINATION | 2020M-162

Town of Clifton Park

Information Technology

NOVEMBER 2021

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

Contents

Report Highlights

Town of Clifton Park

Audit Objective

Determine whether Town of Clifton Park (Town) officials adequately safeguarded information technology (IT) resources.

Key Findings

Officials did not adequately safeguard IT resources. Although the Town paid an IT service provider more than $98,000 in 2019, officials did not define the provider's responsibilities.

Specifically, officials did not:

- Establish a comprehensive IT policy or monitor employee Internet use.
- Implement comprehensive procedures for managing, and monitoring user access to, the Town's network and computers. Fourteen user accounts belonged to former employees who left Town employment one month to 15 years before our review.
- Have a written contract with the Town's IT provider that described specific services to be provided.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Ensure compliance with IT policies.
- Develop comprehensive written procedures for managing and monitoring network user accounts.
- Develop a written IT service level agreement.

Town officials disagreed with certain aspects of our findings and recommendations, but indicated they have initiated corrective action. Appendix B includes our comments on issues raised in the Town's response letter.

Background

The Town is located in Saratoga County. It is governed by an elected Town Board (Board) composed of a Town Supervisor (Supervisor) and four Board members.

The Board is responsible for the general oversight of the Town's operations and finances, which includes maintaining security over the Town's IT system.

Town officials contracted with an IT provider for IT services, including IT support, network management and other IT-related services.

The Town relies on its IT system for Internet and email access and accessing financial data and applications that reside within its IT network.

Quick Facts	
Network Accounts	129
Computers (Desktops, laptops)	72
Employees	137

Audit Period

January 1, 2019 – February 29, 2020. We extended our scope period to March 11, 2020 for IT information collection.

Information Technology

How Should IT Resources Be Safeguarded?

A town board should establish computer policies that take into account people, processes and technology. Each town's unique computing environment should dictate the content of policies.

Computer policies should include clear guidelines and information related to Internet, email and personal computer use; use of and access to personal, private and sensitive information (PPSI)[1]; and password security. The Board should ensure IT policies are communicated to all Town officials, employees and the Town's IT provider. The Board required all IT users to sign an acknowledgment form indicating they had read, or would read, and comply with the Town's IT policy, which was included in the employee handbook.

In addition, the Board should ensure officials monitor employees' computer use to ensure they are complying with the Town's computer policies. Monitoring for compliance with adopted policies involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Automated mechanisms, such as web filtering software, 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.

…[T]he Board should ensure officials monitor employees' computer use to ensure they are complying with the Town's computer policies.

Officials Did Not Monitor Employee Internet Use

Although officials set up web filtering software to prevent access to certain websites, including web mail, they did not monitor employee Internet use. Also, officials did not implement procedures to monitor compliance with the IT policy related to personal use of the Town's communication systems and equipment.

In addition, the IT policy was vague in its definition of acceptable employee Internet use. It stated that "incidental" and "occasional" nonbusiness use was acceptable but did not define those terms. Consequently, this placed the responsibility for determining the reasonableness of personal Internet use on the employees themselves.

The IT policy prohibited personal use of the communication systems and equipment that interferes with employees' performance and indicated that any employee who violated the policy would be subject to disciplinary action up to, and including, termination of employment. However, because officials did not monitor employee Internet use, they could not determine whether it was interfering with productivity or whether it was appropriate to take disciplinary action.

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 reviewed 11 network user accounts[2] on 11 computers assigned to 10 employees[3] and found personal Internet use on all 11 computers, including one that was used to access sports betting websites, which was prohibited by the Town's IT policy. The employees also accessed websites for personal commercial purposes, such as shopping and banking, and browsing entertainment news, sports, blogs, social media, travel and vacation websites (Figure 1).

Figure 1: Examples of Personal Internet Use

Type	Website
Entertainment	cafewell.com, dollywood.com, allrecipes.com, cookinglight.com, disneyplus.com, divorcepayday.com, espn.com, yelp.com, youtube.com
News media	cnn.com, dailygazette.com, foxnews.com, mercurynews.com, news10.com, timesunion.com
Personal email	mail.google.com, mail.yahoo.com, webmail.spectrum.net
Personal online banking	bank.mtb.com, citizensbank.com, edwardjones.com, key.com, paypal.com, pioneerbanking.com, retire.massmutual.com, tdameritrade.com, truelivingfinancial.com
Social media	facebook.com, twitter.com, pinterest.com
Shopping	amazon.com, ebay.com, joann.com, kohls.com, llbean.com, lowes.com, shop.lululemon.com, sixflags.com, target.com
Travel	flightaware.com, jetblue.com, southwest.com, wadetours.com

In addition, we reviewed available acknowledgment forms for the 10 employees and found that one had not signed a form. Although the account user who accessed sports betting websites signed the acknowledgment form, he still violated the policy. When IT users do not sign an acknowledgment form, the Town has an increased risk that IT users will be unaware of the Town's IT policy and its requirements, which increases the risk that the Town's IT systems and data could be exposed to loss or misuse.

Internet browsing and personal use of Town computers increases the likelihood of exposing computer systems to malicious content that could compromise PPSI or the IT system. The Town's failure to adequately protect PPSI can have significant consequences, such as causing damage to its reputation, having legal action initiated against it by those affected by unauthorized distribution of PPSI, disrupting Town operations and/or suffering a security breach of the Town's IT system.

The Town's failure to adequately protect PPSI can have significant consequences...

2 Network user accounts are those accounts that are stored on a centralized server and can be used to log onto multiple computers on the network.

3 These 11 accounts were assigned to 10 Town officials and employees. Refer to Appendix C for more information on our sample selection.

How Should Officials Manage User Accounts and Permissions?

User accounts enable networks and computers to recognize specific users, grant appropriate user permissions and provide user accountability by associating user accounts with specific users. 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 IT data and assets are protected from unauthorized use and/or modifications. 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 employees leave Town employment or when user accounts are no longer needed, these user accounts should be disabled in a timely manner. When employees transfer to another area or have other changes in work functions, their accounts should be reviewed and permissions adjusted accordingly. Town officials should develop written procedures for granting, changing and removing user access and permissions to the overall networked computer system and to specific computers, applications and folders.

Generally, administrative accounts have oversight and control of networks, 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 network or local administrative permissions runs will inherently run with the same permissions. For example, if malicious software (malware) 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 network or computer compromise and/or data loss. Officials must limit administrative permissions to those users who need them to complete their job functions.

Officials must limit administrative permissions to those users who need them to complete their job functions.

Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if necessary.

Officials Did Not Implement Strong Access Controls

Town officials have not implemented comprehensive procedures for managing and monitoring user access to the Town's network and computers. The IT

provider configured and maintained the Town's IT environment, which included servers, desktops, network accounts and software applications. Town officials communicated their needs and requests to the IT provider through phone calls, emails or in person.

We reviewed the Town's 129 network user accounts and found unneeded user accounts and accounts that had unneeded administrative permissions and access to accounting records, as follows:

Unneeded User Accounts – We found that 25 network user accounts (19 percent) were unneeded, as follows:

- Fourteen accounts belonged to former Town employees who had left Town employment ranging from one month to 15 years before our review. However, the IT provider did not disable these accounts, and they were still active. Nine of the accounts had never been used to log onto the network.
- Nine other accounts were generic accounts, three of which had unneeded administrative permissions.[4]
- Another user account was used for a legacy system, which was no longer in use, and had unneeded administrative permissions.[5]
- Another user account was assigned to an individual who was using it as a second account. This account also had unneeded administrative permissions.[6]

Because the Town did not have procedures in place to periodically review all network user accounts, these unneeded accounts went unnoticed. When unneeded network user accounts exist, the Town has an increased risk that disgruntled former employees or other attackers could use these accounts as entry points to access PPSI and compromise IT resources.

Of particular risk are the accounts belonging to former employees because their existence indicates the Town has inadequate account maintenance and monitoring. Without adequate account maintenance, the Town has an increased risk that attackers could successfully compromise its IT system. Also, because network user accounts were not monitored, the Town has a greater risk that the IT provider would not notice if the accounts had been compromised or used for malicious activities, which would give attackers more time and opportunities to access PPSI and compromise the Town's IT resources.

4 The three unneeded generic accounts with unneeded administrative permissions are also mentioned in the Unneeded Administrative Permissions section.

5 This account is also mentioned in the Unneeded Administrative Permissions section.

6 The three generic accounts with unneeded administrative permissions, the account used for a legacy system and the second account with unneeded administrative permissions (last list item) are mentioned in the Unneeded Administrative Permissions section.

Unneeded Administrative Permissions – We found that 17 accounts (13 percent) were unnecessarily assigned administrative permissions, as follows:

- Nine belonged to Town officials and employees who did not need administrative permissions to perform their job duties.
- Seven were generic accounts, of which three were unneeded accounts.
- One was used for a legacy system and was an unneeded account.[7]

When employees have unnecessary administrative permissions, the Town has an increased risk that unauthorized changes could occur or PPSI could be used inappropriately. Also, the compromise of an account with administrative permissions could cause greater damage than with a lesser-privileged account because these accounts have full control over the network or user computers. Consequently, the Town's IT resources and data are at increased risk for loss or misuse.

Unneeded Access – We found that three network user accounts had unneeded access to a network folder that was assigned to the Town's accounting department. Two belonged to employees who transferred to different Town departments in 2015 and 2018 and no longer needed access to this folder. The remaining account belonged to a former employee who left Town employment in 2005.

Because the Town did not have procedures in place to periodically review all network user accounts, this unneeded access went unnoticed. As a result, the Town has an increased risk that unauthorized users could manipulate or delete data.

Why Should the Town Have a Written Contract and Service Level Agreement (SLA) With its IT Provider?

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. To avoid potential misunderstandings and to protect Town assets, officials should have a written contract between the Town and its IT provider that clearly states the services to be provided, when they will be provided, how they will be provided and at what cost. The contract should require the IT provider to have a system of internal controls in place to provide reasonable assurance that the Town's information will be protected against loss, abuse and fraudulent activity.

7 The three unneeded generic accounts and one used for a legacy system also are mentioned in the Unneeded User Accounts section.

In addition, officials should have a written SLA between the Town and its IT provider that identifies the Town's needs and expectations and specifies the level of service to be provided. 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.

SLAs provide 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. Having a written contract and SLA with the IT provider will allow officials to monitor the IT provider's work to ensure that the Town is receiving all contracted services.

Having a written contract and SLA with the IT provider will allow officials to monitor the IT provider's work…

The Town Did Not Have a Written Contract or SLA With its IT Provider

The Town has relied on an IT provider for IT services for more than five years and paid more than $98,000 in 2019 for these services. The IT provider provided software; hardware equipment; software, network and Wi-Fi support; server, workstation, firewall and router maintenance; data wiring; backup services; and other IT services. However, during our audit period, officials did not have a written contract with the IT provider that identified the IT provider's responsibilities or the specific services to be provided.

…[O]fficials did not have a written contract with the IT provider that identified the IT provider's responsibilities or the specific services to be provided.

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

Without a formal written contract and SLA, officials were unaware of the extent of services being provided and could not ensure the Town was receiving the services to which it paid for and should have received. Insufficient, nonexistent or vague agreements can contribute to confusion regarding who is responsible for various aspects of the IT environment, including data recovery in the event of a ransomware[8] attack or other security incident, which puts data and computer resources at greater risk for unauthorized access, misuse or loss.

8 Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Why Should the Town Have a Disaster Recovery Plan?

A disaster recovery plan (plan) provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. To minimize the risk of data loss or suffering a serious interruption of services, town officials should establish a formal written plan. This is particularly important given the current and growing threat of ransomware attack. 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 availability or integrity of town services, including the IT system and data.

Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary precautions needed to maintain or quickly resume operations. The plan should be periodically tested and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements. Additionally, a plan should include data backup procedures and periodic backup testing to ensure they will function as intended.

Officials Did Not Adopt a Disaster Recovery Plan

Town officials did not develop, adopt or implement a disaster recovery plan to describe how officials would respond to potential disasters. On a daily basis, computers connected to the network are backed up to the server, and the backups are tested by the software backup application and uploaded to cloud-based storage.[9] However, the Town does not have any guidelines in place to delegate responsibilities or minimize effects to operations in the event of a disaster. Town officials acknowledged they did not have a plan and told us they intended to create one within the next year while updating Town policies and procedures.

Without a disaster recovery plan, officials cannot guarantee that in the event of a disaster they would be able to restore critical IT systems, applications or data in a timely manner. Depending on the severity of an incident, officials may need to expend significant time and financial resources to resume Town operations.

…[O]fficials cannot guarantee that in the event of a disaster they would be able to restore critical IT systems, applications or data in a timely manner.

9 Cloud-based storage makes it possible to save files to a remote storage location and retrieve them on demand.

Furthermore, essential employees may not be aware of their roles, which could complicate the Town's ability to recover from an incident. As a result, 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.

What Do We Recommend?

The Board should:

1. Update IT policies to provide clear guidance for personal and prohibited use of IT computer systems and equipment.
2. Enter into a formal written contract with the IT provider that sufficiently defines the contractual relationship and responsibilities between the IT provider and the Town.
3. Develop an SLA with the IT provider that addresses the Town's specific needs and expectations for IT services.
4. Develop and adopt a comprehensive disaster recovery plan.

Town officials should:

5. Implement procedures to monitor employee Internet use to ensure compliance with IT policies.
6. Ensure all IT users sign a form acknowledging that they are aware of and will comply with the Town's IT policies.
7. Develop comprehensive written procedures for managing and monitoring network user accounts that include periodically reviewing user access and disabling or changing accounts when access is no longer needed.
8. Ensure the IT provider immediately disables the network user accounts of former Town employees.
9. Ensure the IT provider removes unneeded administrative permissions granted to user accounts and periodically review administrative permissions to ensure they are appropriate for users' job functions.
10. Ensure the IT provider removes the unneeded user access to the Town's accounting department folder identified in this report.
11. Become familiar with the services provided by the IT provider and ensure the Town receives the services to which it is entitled.

Appendix A: Response From Town Officials

Town of Clifton Park

One Town Hall Plaza | Clifton Park, New York 12065 | (518) 371-6651 | Fax: (518) 371-1136

September 7, 2021

[redacted]
NYS Office of the State Comptroller
Division of Local Governments
One Broad Street Plaza
Glens Falls, N.Y. 12801

On behalf of the Town of Clifton Park, we thank the NYS Comptroller's Office for reviewing the Town's IT system and usage. IT upgrades are increasingly important. When I first began my tenure as Town Supervisor, the Town did not have a professional, interactive website, which was soon corrected. From that point in time to today, the Town has made tremendous strides to protect and store data and keep pace with technological advances in software and hardware needs.

In recent years we have invested a significant amount of money in a full server system upgrade that provides redundancy, off site data storage and a hardened IT system. We have also replaced our computer equipment for each employee and upgraded all software licenses. We have completed many other upgrades and some are referenced in this document.

As far as the Key Findings of the report are concerned, please see the following responses.

Key Finding 1: The Town did not adequately safeguard IT resources because we paid our IT consultant $98,000 in 2019 without defining the providers responsibilities.

Response: The actual expenditure for consulting services during the audit period was $48,100, with the remaining funds expended for purchases of hardware and software, cloud-based backup service and installation expenses. All payments made to IT consultants for services, or any other expense related to IT is approved by the Town Board or included in an agreement. A staff person assigned to oversee IT matters also provides vetting for all expenses prior to approval by my office. Further, our consulting arrangement with ABS is comprehensive. In 2020, the town entered into a written agreement with ABS, approved by the Town Board, wherein ABS agreed to provide comprehensive services to the Town. The agreement defines an hourly rate, and the company provides plenary support to all departments through my office.

See Note 1 Page 13

The Town declined to pre-pay for professional services in order to receive an upfront guarantee on service response time. ABS typically does not provide customers with specific service level agreements as the hardware and equipment is owned by the customer and the customer provides basic system management. ABS does not guarantee service levels on Town-owned equipment.

However, throughout the Town's 6 year relationship with our current IT consultant, ABS Solutions has consistently provided prompt, reliable and affordable IT Services and the Town is able to terminate the agreement with a 30 day notice at any time if we become unsatisfied with

their performance, solutions offered, or response times. These are business decisions that fall within the Town's discretion.

Furthermore, an informal survey of surrounding municipalities shows that our overall expenditure on IT consulting services compares favorably with our peers, in some cases significantly, further reinforcing our determination articulated above.

Key Finding 2: We did not have a comprehensive internet policy.

Response. This is also not accurate. Our Internet policy is included in the employee manual, which has been prepared by our HR consultants, who have scores of municipal clients throughout the Capital Region. The policy in our manual is standard to the vast majority of our consultant's clients and is consistent with those entities.

See Note 2 Page 13

Key Finding 3: We did not have a written contract with our IT consultants that described specific services to be provided.

Response: See above. Our current contract with ABS is dated June 24, 2020. Our relationship with ABS during the 2019 audit period was defined by Purchase orders for specific projects as well as a clearly defined hourly rate.

See Note 1 Page 13

Key Finding 4: Implement comprehensive procedures for managing and monitoring user access to the Town's network and computers. Fourteen user accounts belonged to former employees who left Town employment one month to 15 years before our review.

Response: It is important to note a number of the identified "former" employees remain active with the Town. Any unnecessary accounts have been disabled. Further, the email accounts for these individuals were not operable and none of these individuals had or have remote access to the Town's system. Any usage affiliated with their account would need to be accomplished through electronic devices, which are all in secure areas. In 2019, we began implementing a system that automatically disabled an account that is not used. We will review our accounts quarterly to ensure there are no accounts that are unnecessarily active.

See Note 3 Page 13

The Town has also implemented [redacted] Total Email Protection. [redacted] provides the Town with [redacted] backup and monitoring. Any email sent through [redacted] has [redacted] Technology that sandboxes all weblinks. Lastly, advanced antivirus software with application control is also in place.

It is important to note, the Town's upgrades for data security ensure our data is protected in an emergency situation or disaster. The time frame and resources necessary to restore system viability for Town operations, will depend solely on the type of emergency we experience. One of the quotes in the report states, "Officials cannot guarantee that in the event of a disaster they would be able to restore critical IT systems, applications or data in a timely manner." That quote is absolutely accurate as there is no possible way to place a time frame on restoration, without knowing the extent of the severity of the disaster.

The report also listed a number of "questionable" websites that were visited by Town employees. A majority of the sites are useful and reasonable for Town employees to use during the course of conducting business. Purchasing activities, financial tasks, travel and trip destination research and many other normal Town functions require usage of related sites. We periodically send reminders to all employees about phishing attacks and other issues involving computer use. Do we closely monitor the usage of each employee on a regular basis? No. Do we monitor and survey computer usage when we believe there is a reason to do so? Yes. We record all web traffic. We also have a product that blocks all web mail access through the Town computers, eliminating the opportunity to utilize the system for personal email.

See Note 4 Page 13

The information included in this response will be helpful to you and anyone interested in the IT systems of the Town. We understand the use of boiler plate language in the audit reports for headline purposes. I am pleased there was nothing identified in the audit that would cause alarm, or place the Town systems in a compromised position, nor has the door been opened to abuse or unwarranted entry. We will continue to fortify our systems and enhance our technological capabilities. It is very challenging for any organization to keep pace with the lightning quick advances that occur in the area of IT each year. The Town of Clifton Park, as a moderately sized organization, has done a tremendous job ensuring advanced technologies are implemented to protect and store data, important security protections are installed, new hardware and software is provided to promote employee productivity, policies are implemented and other very important upgrades. As the auditors know, we were in the midst of some significant upgrades when the audit began and we have implemented many system changes since they arrived. Upgrading IT is a never ending job and there is always more that can be implemented as new technologies and products appear daily.

See Note 5 Page 13

See Note 6 Page 13

Sincerely,

Phil Barrett
Town Supervisor

Appendix B: OSC Comments on the Town's Response

Note 1

The Town paid the IT provider more than $98,000 in 2019 for software; hardware equipment; software, network and Wi-Fi support; server, workstation, firewall and router maintenance; data wiring; backup services; and other IT services. However, the Town did not have a written contract or SLA with the IT provider during our audit period.

Note 2

The Town's IT policy did not provide a clear definition of acceptable employee Internet use.

Note 3

None of these 14 accounts belonged to active Town employees. When employees leave Town employment or when user accounts are no longer needed, these user accounts should be disabled in a timely manner. Attackers could use accounts belonging to former employees to successfully compromise the Town's IT system and, because of inadequate account maintenance and monitoring, the IT provider would not notice if the accounts had been compromised or used for malicious activities, which would give attackers more time and opportunities to access PPSI and compromise the Town's IT resources.

Note 4

Employees' web history had clear patterns of personal Internet use that was shown by the information that they searched for and accessed. Internet browsing and personal use of Town computers increases the likelihood of exposing computer systems to malicious content that could compromise PPSI or the IT system. The Town's failure to adequately protect PPSI can have significant consequences, such as causing damage to its reputation, having legal action initiated against it by those affected by unauthorized distribution of PPSI, disrupting Town operations and/or suffering a security breach of the Town's IT system.

Note 5

Both the public and confidential audit reports identified numerous significant deficiencies in safeguarding IT resources. As a result, the Town has a greater risk that its IT resources could be accessed by unauthorized individuals, user accounts could be compromised and malicious activity could occur.

Note 6

We considered all system changes made during our audit period.

Appendix C: Audit Methodology and Standards

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

- We interviewed Town officials, employees and the IT provider to obtain an understanding of the Town's IT environment, internal controls and applicable processes, procedures and applications. We also determined whether the Town had any IT policies and whether Town personnel received any IT security awareness training.
- We reviewed the written agreement between the Town and the payroll vendor to gain an understanding of the services provided and controls in place to protect the Town's financial assets.
- We reviewed the Town's employee handbook to identify IT policies related to acceptable personal and prohibited IT and computer use.
- We used our professional judgment to select 10 officials and employees based on their job titles and duties, which included accessing the Town's accounting system, performing online banking activities and troubleshooting minor IT issues for employees. The 10 employees were assigned 11 network user accounts and used 11 computers. We reviewed these employees' Internet activity and determined whether the Town had signed acknowledgement forms on file for all 10 of them.
- We analyzed and assessed all 129 network user accounts and the server with the domain controller and analyzed shared folders on the Town's servers using a specialized audit script.
- We compared the results of our network user account analysis to the Town's employee list to determine whether there were any active user accounts still assigned to former Town employees.

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.

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 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 D: Resources and Services

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

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

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

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

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

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

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

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

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

Contact

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

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

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

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

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

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