REPORT OF EXAMINATION | 2022M-9

Town of Minetto

Information Technology

MAY 2022

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

Contents

Report Highlights

Town of Minetto

Audit Objective

Determine whether Town of Minetto (Town) officials ensured information technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

Town officials did not ensure IT systems were adequately secured and protected against unauthorized use, access and loss. In addition to sensitive IT control weaknesses that were communicated confidentially to officials, the Town Board (Board) and officials did not:

- Provide IT security awareness training to all computer users.
- Adequately manage local user accounts and permissions. As a result, four of 10 computers had unneeded and unused local user accounts.
- Adopt written procedures for user accounts or a comprehensive written IT contingency plan to minimize the risk of data loss or suffering a serious interruption of service.

Key Recommendations

- Provide periodic IT security awareness training to all personnel who use Town IT resources.
- Ensure user accounts and permissions are regularly reviewed and unnecessary accounts are disabled in a timely manner.
- Adopt written procedures for user accounts and permissions and a comprehensive written IT contingency plan.

Town officials generally agreed with our findings and recommendations and indicated they planned to take corrective action.

Background

The Town is located in Oswego County and is governed by an elected Board that is composed of the Town Supervisor (Supervisor) and four Board members.

The Board is responsible for the general oversight of the Town's operations and finances, which includes establishing policies and procedures to help protect IT systems and provide a secure IT environment. The Supervisor is responsible for the Town's day-to-day activities.

Town employees and officials use the Town's IT systems for Internet access and email, and to maintain various records such as financial and personnel records and Justice Court case files.

Quick Facts	
Employees	24
Computers	10
Local User Accounts	20

Audit Period

January 1, 2020 – October 6, 2021

Information Technology

The Town relies on its IT systems for maintaining financial and personnel records and Justice Court (Court) case files, and for email and Internet access. Some of the records and files maintained by the Town's IT systems contain personal, private and sensitive information (PPSI). PPSI is any information that 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. If the Town's IT systems are compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and rebuild. While effective controls will not guarantee the safety of an IT system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

The Town has seven computers used by various Town officials and employees, and the Court has three computers used by the Town Justice (Justice) and court clerk. The Court computers were provided by the New York State Unified Court System's (UCS) Office of Court Administration (OCA).[1] While OCA plays a role in supporting and updating the Court's computers, Town officials are ultimately responsible for ensuring the necessary IT controls are in place to secure the Town's IT systems and the computers that connect to its network. As such, the Justice should work with OCA to address the IT security weaknesses we identified for the Court computers.

Why Should the Board Adopt IT Policies and Provide Security Awareness Training?

IT policies describe the tools and procedures used to help protect data and IT systems, assign key responsibilities, define the board's expectations for appropriate user behavior and explain the consequences of policy violations. A board should provide oversight and leadership by adopting written IT policies that take into account people, processes and technology and should communicate the policies to all computer users.[2] Further, a board should periodically review these policies, update them as needed and designate personnel who are responsible for monitoring policy compliance.

New York State Technology Law Section 208 requires towns to have a breach notification policy. This policy must require that notification be given to certain individuals when there is a security breach of the system related to private

1 OCA is the administrative arm of UCS. The Division of Technology is a unit within OCA that provides technology services for UCS, including town and village courts.

2 For additional guidance on recommended IT policies refer to our *Local Government Management Guide – Information Technology Governance* at: https://www.osc.state.ny.us/files/local-government/publications/pdf/itgovernance.pdf.

information. A board should also adopt an acceptable computer use policy (AUP) that defines what constitutes appropriate and inappropriate computer, Internet and email use and specific consequences for violations.

In addition, a board should adopt a password security policy. This policy should address the board's expectations for password complexity, length, age requirements and the number of failed log-on attempts the system will allow. Strong password controls improve the chances that unauthorized users will be prevented from accessing the town's computers and data.

Furthermore, to minimize the risk of unauthorized access and misuse or loss of data and PPSI, the board should ensure periodic IT security awareness training is provided to all computer users explaining the proper rules of behavior for using the Internet and IT resources, systems and data. The training should communicate related policies and procedures to all users so they understand IT security measures and their roles in safeguarding data and IT assets. For example, the training should cover key security concepts such as the dangers of downloading files and programs from the Internet; the importance of selecting strong passwords; requirements related to protecting PPSI; and how to respond if a virus or an information security breach is detected. In addition, board members should participate in ongoing IT security training to stay aware of current trends to ensure they have appropriate policies in place and are able to keep them updated as needed.

The Board did not adopt written IT policies during our audit period or in prior years.

The Board Did Not Adopt IT Policies or Ensure Security Awareness Training Was Provided

The Board did not adopt written IT policies during our audit period or in prior years. Therefore, it did not provide adequate guidance and direction to address key IT security issues, such as acceptable use, passwords and breach notification. Furthermore, the Board did not ensure IT security awareness training was provided to officials and employees who use Town and Court computers.

Because the Board did not adopt an AUP governing appropriate use of IT assets and provide employees with IT security awareness training, we reviewed the Internet browsing histories on all 10 Town and Court computers.[3] We did not identify any significant personal Internet use by officials or employees.

While comprehensive policies will not guarantee the safety of IT assets and data, not adopting policies and providing IT security awareness training significantly increases the risk that users may not understand their responsibilities and are more likely to be unaware of situations that could put Town data and PPSI at

3 See Appendix B for our audit methodology.

greater risk for unauthorized access, misuse and loss. For example, if a user were to inadvertently download a malicious software program from the Internet, or click on a malicious attachment, it could infect the user's computer and potentially other computers connected to the Town's network. This could allow individuals to steal information or gain unauthorized access to sensitive information, such as Social Security numbers and bank account information. Without a breach notification policy, officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals if private information is compromised.

While the Supervisor told us they are aware of the need to adopt comprehensive IT policies and procedures, the COVID-19 pandemic, significant turnover with elected and appointed officials, and other Town matters prevented them from developing the policies and procedures. However, officials should have developed the policies and procedures years ago, prior to the COVID-19 pandemic. After our audit fieldwork, the Board adopted policies to address acceptable use, passwords and breach notification to help strengthen the Town's IT security environment. The Supervisor told us they had not considered the importance of IT security awareness training prior to our audit.

How Should Officials Manage User Accounts and Permissions To Help Protect and Secure IT Systems?

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.

Town officials are responsible for restricting user access to only those applications, resources and data needed to complete job duties and responsibilities.

Local user accounts enable computers and certain applications to recognize specific users and processes, allow system administrators to grant appropriate permissions and provide user accountability by affiliating user accounts with specific users and processes.

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

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

Additionally, users with local administrative permissions may run programs with the same higher permissions. For example, if malicious software installed itself on a computer, it could 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 should limit local administrative permissions to those users and processes who need them to complete their job duties and functions.

> …[T]he Justice could not explain the purpose of all 12 local user accounts on the Court's three computers.

Officials Did Not Adequately Manage User Accounts and Permissions

The Board did not adopt written procedures for granting, changing or disabling access to Town and Court computers. Additionally, officials did not periodically review local user accounts to ensure the accounts were necessary and the permissions were needed. As a result, one of the Town's computers and all three Court computers had unneeded and unused local user accounts that were not disabled.

We examined 20 local user accounts on 10 computers and found one account with administrative privileges on the Town Clerk's computer that was unnecessary and should have been disabled. The Supervisor told us he was unaware that the Town Clerk's computer had an additional local user account that should be disabled.

Additionally, the Justice could not explain the purpose of all 12 local user accounts on the Court's three computers. Eleven of these 12 local user accounts have administrative privileges. In addition, seven of the local user accounts have either never been used or were last used in 2013.

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

Why Should the Board Adopt an IT Contingency Plan To Help Protect and Secure IT Systems?

An IT contingency plan is a town's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT disruption. An unexpected IT disruption could include a power outage, software failure caused by a virus or other type of 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, length and resources necessary to prepare an IT contingency

plan will vary depending on the size and sophistication of the town's operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident and could significantly reduce the resulting impact.

The goal of an IT contingency plan is to enable the recovery of an IT system and/or electronic data as quickly and effectively as possible following an unplanned disruption. Because IT often supports key business processes, planning for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining a town'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 town, 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, and
- Details concerning how the plan will be periodically tested and updated.

The goal of an IT contingency plan is to enable the recovery of an IT system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

The Board Did Not Adopt an IT Contingency Plan

The Board did not adopt a comprehensive written IT contingency plan to describe the procedures and technical measures officials would take to respond to potential disruptions affecting IT. Officials were unable to provide a reasonable explanation for not having a written comprehensive IT contingency plan in place.

Consequently, in the event of a disruption or attack (e.g., ransomware), Town officials and employees have insufficient written guidance to restore or resume essential operations in a timely manner and help minimize damage and recovery costs. In addition, 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.

What Do We Recommend?

The Board should:

1. Periodically review and update the recently adopted IT policies and establish procedures to ensure compliance.
2. Ensure IT security awareness training is periodically provided to all individuals who use Town IT resources and attend the training to stay aware of current security risks.
3. Develop and adopt written procedures to address user accounts and permissions.
4. Ensure user accounts and permissions on Town computers are reviewed on a regular basis and any unnecessary accounts are disabled in a timely manner.
5. Adopt a comprehensive written IT contingency plan that provides specific guidance for the protection of IT assets and data against loss or destruction. Ensure that the plan is periodically tested and updated.

The Justice should:

6. Regularly review all local user accounts and permissions on Court computers and work with OCA to restrict permissions or disable any accounts deemed unnecessary.

Appendix A: Response From Town Officials

TOWN OF MINETTO
6 COMMUNITY DRIVE
P.O. BOX 220
MINETTO, NEW YORK 13115-0220
315 • 343-2393 Fax: (315) 342-4421

May 12, 2022

Rebecca Wilcox, Chief Examiner
Office of the NY State Comptroller
Division of Local Government & School Accountability
PSU – CAP Submission
110 State Street 12th Floor
Albany, NY 12236

Dear Ms. Wilcox,

I am writing in response to the Information Technology audit conducted by your department. We would like to thank you for conducting this audit of the Town of Minetto. Prior to the arrival of your staff, we recognized the need for a major IT overhaul. We had sought proposals and pricing from several companies to conduct a study of the town's IT systems, etc. with the goal of modernizing our entire process. The audit conducted by your agency aided us in focusing our IT overhaul on the key items that were needed.

We are in complete agreement with the audit findings and recommendations.

We have embraced the audit findings and have responded with corrective action for each recommendation. Nearly all items have already been completed. It is our intent to adopt all the recommendations.

Just two items remain. The necessary IT training and the development and adoption of an IT contingency plan. Most recently, we have selected an online IT training course. We have assigned this training to our staff, and it will be completed in the next 30 days.

We are continuing with the development of an IT contingency plan. This is a complicated undertaking. We are actively progressing through the development phase of this plan, and we are confident the task will be accomplished soon.

I would like to close by addressing your staff's performance during the audit period. As someone who has been involved in supervision and management for over 40 years, I feel strongly that excellent employees deserve to be recognized. It has been clear to me throughout the audit process that your auditors are hard working dedicated employees who enjoy what they do and are especially talented at assisting others. On several occasions, the auditor's willingness to assist us resulted in our ability to make immediate changes which enhanced our security and improved operations while the auditors were still onsite!

Thank you!

John Famiilo
Town Supervisor

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, our audit procedures included the following:

- We interviewed officials and employees and reviewed Town records to obtain an understanding of the Town's IT operations.
- We inquired whether the Town had written IT policies or procedures or an IT contingency plan.
- We ran a computerized audit script between September 21 and October 6, 2021 on 10 computers used by Town officials or employees (seven Town computers and three Court computers). We then analyzed the results generated by the scripts to obtain information about the computers' local user accounts, including their permissions and security settings, to determine whether the user accounts were necessary and the security settings applied to the user accounts were consistent with industry standards. We then asked Town officials about inactive and potentially unneeded local user accounts and security settings that were inconsistent with industry standards.
- We ran a web history computerized audit script on the 10 computers and reviewed the web history to evaluate whether Internet use was appropriate and if unnecessary exposure of PPSI had occurred.

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

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/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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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