REPORT OF EXAMINATION | 2020M-137

Town of New Windsor

Information Technology

APRIL 2021

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

Contents

Report Highlights

Town of New Windsor

Audit Objective

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

Key Findings

Town officials did not:

- Provide employees with cybersecurity training.
- Have a disaster recovery plan.
- Ensure online banking agreements comply with New York State General Municipal Law (GML).

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

Key Recommendations

- Provide employees with periodic IT security awareness training.
- Develop a comprehensive, written disaster recovery plan that provides specific guidelines for the protection of IT assets and data against loss or destruction.
- Ensure online banking agreements comply with GML, and that those who perform online banking transactions are familiar with its content.

As indicated in Appendix A, officials disagreed with several of the findings and recommendations in our report. Appendix B includes our comments on the issues raised in the Town's response letter.

Background

The Town, located in Orange County, NY, is governed by an elected Town Board (Board) that is composed of four council members.

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 Chief of Information Technology (CIT) is responsible for managing the Town's IT department. The CIT, along with a Deputy CIT and two information technology officers, oversee the Town's IT activities and provide support for IT operations.

In addition, the IT Department provides IT support services to more than 15 local municipalities throughout Orange County, NY.

Quick Facts	
Employees	213
Network Accounts	226
2019 Budgeted Appropriations – IT Department	$977,000

Audit Period

January 1, 2018 – November 21, 2019. We extended our audit period forward through March 11, 2020 to complete our IT testing.

Information Technology

The Town relies on its IT assets for Internet access, email, and for maintenance of financial, personnel and taxpayer records, much of which contains personal, private or sensitive information (PPSI). If the IT system is compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer 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.

How Does an Acceptable Use Policy (AUP) Protect IT Systems?

The town should have an AUP that defines the procedures for computer, Internet and email use. The policy should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy. In addition, officials should require employees to sign acknowledgement forms to indicate they have read the town's AUP and are aware of what is expected of them and to acknowledge they will be held accountable for compliance with the policies and procedures outlined in the AUP.

Officials Did Not Have Signed Agreement/Acknowledgement Forms for the Town's AUP

Although the Town has an AUP included in the "Employee Handbook for Information Technology Security," adopted in September 2013 that requires employees to sign an "Employee Information Security Policy Agreement (Agreement)" form, Town officials could not provide the forms for any of their network users. Per the Town's employee handbook concerning information technology security, these forms serve as record that the intended party has read, understands and is aware of their responsibility while accessing and using Town resources as well as where to find these policies. The scope of these policies, according to the manual, consists of all parties, including outsourced and third-parties with access to and/or management of Town information systems and data resources.

We requested signed Agreement forms for a sample of 10 employees, and officials provided us with outdated AUP forms, from the Agreement adopted in 2005, signed by nine of the 10 employees. However, officials did not obtain signed copies of the updated Agreement forms when they updated the handbook in 2013. According to officials, there was confusion over employee Agreement/acknowledgement forms and who was responsible for the distribution and collection of these forms.

Without the use of signed Agreement forms, officials cannot be assured that all network users are aware of and have acknowledged to abide by Town IT policies and procedures. In addition, employees may not know what constitutes appropriate and inappropriate behavior or best practices as it relates to security controls implemented by the Town which further increases the potential risk of unauthorized access, use and loss of data including PPSI.

Why Should 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 accessing IT systems and data. In addition, the training should communicate related policies and procedures to all employees so they understand IT security measures and their roles in safeguarding data and IT assets.

The training should center on emerging trends such as information theft, social engineering attacks and computer viruses and other types of malicious software, all of which may result in PPSI compromise or denying access to the IT system and its data. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

Officials Did Not Provide Cybersecurity Awareness Training

Town officials did not provide users with IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets. Officials stated that the IT department periodically provided technical memos. However, officials cannot substantiate or wholly support that these memos were received, read by and understood by the intended recipients.

Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, Town data including PPSI could be at greater risk for unauthorized access, misuse and loss.

Why Should the Town Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, 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 systems, data and PPSI contained therein.

Typically, a plan involves analyzing business processes and continuity needs, identifying critical IT systems, software and the roles and/or responsibilities of key individuals necessary to maintain or quickly resume operations. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements, systems/equipment and personnel.

Officials Did Not Have a Disaster Recovery Plan

Town officials did not develop a comprehensive written plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster, officials have no guidelines or guidance to minimize or prevent the potential loss of equipment and data. While officials acknowledged they did not have a plan, officials were in the process of updating Town policies and procedures and intended to create one.

Without a formal 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. 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.

How Can Officials Protect Online Banking Transactions?

Online banking allows users to access their bank accounts to review current account balances and account information and transfer money between bank accounts and to external accounts. Because funds transferred electronically typically involve significant amounts of money, officials must control the processing of its electronic transfers to help prevent unauthorized transfers from occurring.

New York State General Municipal Law (GML)[1] allows the towns to disburse or transfer funds by electronic transfers, provided that the board enters into a written agreement with the town's bank. GML requires that this agreement describe the manner in which electronic transfers will be accomplished and identify the

1 GML, Article 2, Section 5-A

names and numbers of bank accounts from which transfers may be made and the individuals authorized to request transfers. Also, GML requires towns to implement a security procedure that includes verifying that payment orders are for the initiating town and reviewing payment orders to detect errors in transmission or content.

The board also should adopt an online banking policy that describes authorized online banking activities, specifies which employees are authorized to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of online transactions and describes what type of computing devices should be used to perform online banking transactions. Officials should check with their banks about enabling alerts and other security measures that may be available, such as blocking wire transfers to foreign countries, sending email notifications of electronic transfers and requiring verification of transactions over certain amounts.

To the extent possible, authorized users should access bank accounts from one computer dedicated for online banking from a wired network to minimize exposure to malicious software. Officials could limit the software installed on that computer to programs needed for online banking activities. Online banking should not be conducted from personal devices because officials cannot monitor these devices or ensure they are secure.

Officials Did Not Adequately Safeguard Online Banking Transactions and Online Banking Agreement Did Not Comply with GML

Officials did not have an adequate online banking agreement with the Town's bank. The agreement did not identify the names and numbers of bank accounts from which electronic or wire transfers may be made or identify which individuals are authorized to request an electronic or wire transfer of funds.

The Town also did not have a policy detailing the approval process to verify the accuracy and legitimacy of transactions before they are processed. Officials did not establish security controls such as blocking wire transfers to foreign countries. In addition, employees did not use a dedicated separate computer for online banking activities and were not instructed to access online banking with Town managed and/or approved devices.

Officials stated they were in the process of reviewing policies and procedures including creating an online banking policy. In addition, officials stated they were unaware of GML as it relates to online banking. Without an online banking policy, officials cannot ensure that authorized employees will understand their roles when performing online bank transactions. Furthermore, without an adequate online banking agreement that includes established security controls, officials are significantly increasing the exposure of the Town's bank accounts to unnecessary risk.

It is important to note that each of the findings in this report create a weakness in the Town's controls over information technology. However, when combined these weaknesses can have a compounded effect. For example, not implementing an acceptable use policy and not providing adequate training about cybersecurity leaves employees without any guidance on IT security which increases the risk of malware attack. Since the Town does not have adequate safeguards for online banking, a malware attack could expose the Town to financial loss. Furthermore, if there is a denial of service attack, the Town does not have a disaster recovery plan that would provide guidance to minimize the impact of the attack.

What Do We Recommend?

The Board Should:

1. Adopt an online banking policy that describes authorized online banking activities, specifies which employees are authorized to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of online transactions and describes what types of computing devices should be used to perform online banking transactions.

2. Review, update and adopt an acceptable use policy and establish procedures to ensure compliance.

Officials Should:

3. Ensure that AUPs are distributed as intended and that employee acknowledgement forms are collected for all employee and/or network users.

4. Provide employees with periodic IT security awareness training.

5. Develop a comprehensive, written disaster recovery plan that provides specific guidelines for the protection of IT assets and data against loss or destruction. It should be periodically tested and updated.

6. Ensure that sufficient written banking agreements that address online banking with each bank are in accordance with GML, and that those who perform online banking transactions are familiar with its content.

7. Check with their banks about enabling security measures, such as blocking wire transfers to foreign countries, sending email notifications of electronic transfers and requiring verification of transactions over certain amounts.

8. Designate a computer to be used for online banking transactions.

Appendix A: Response From Town Officials

TOWN OF NEW WINDSOR

555 Union Avenue
New Windsor, N.Y. 12553
Telephone: (845) 563-4602

George J. Meyers, Town Supervisor
Web: http://newwindsor-ny.gov

March 8, 2021

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

Subject: Town of New Windsor Audit 2020M-137

Dear Mr. Auerbach:

I welcome the New York State Comptroller's Office audit review and the Town's operation to ensure efficient constituent services. This letter is the Town of New Windsor's response to the draft audit report into information technology covering January 1, 2018, through March 11, 2020. It also serves as the Town's corrective action plan for the audit's deficiencies.

We disagree with the audit findings that officials did not have signed acknowledgment forms for the Town's AUP. During the audit, we supplied the auditor with 9 out of 10 selected employees signed AUP forms along with the Town's AUP via email due to Covid-19 restrictions. The personnel officer ensures that new employees complete the employment package of documents. The Town's AUP and acknowledgment form is part of the employment packet. We later learned during the exit interview that the auditor never received our email response with the attachment to the auditor. The New York State Comptrollers Office prevents emails with PDF attachments from reaching recipients in their office. We provided the information again

See Note 1 Page 10

to the NYS Comptroller's Office through an alternative means for their review. The revised audit findings state that the Town's AUP is outdated. The Town's AUP accurately represents the policy for the use of Information Technology assets and resources.

We disagree with the audit findings that officials did not provide cybersecurity awareness training. The Town offers continuous cybersecurity awareness training through the Information Technology Department. The Information Technology Department routinely sends out emails, disseminates cybersecurity awareness monthly cybersecurity tips from the NYS Office of Information Technology Services, and personal interaction regarding cybersecurity awareness. We agree that we do not have detailed acknowledgment forms for these learning opportunities. The Town will create the "paper-trail" to acknowledge learning opportunities.

See Note 2 Page 10

We disagree with the audit findings that officials did not have a disaster recovery plan. The Information Technology Department has a disaster recovery plan to safeguard the Town's digital data and assets. The disaster recovery plan follows best practices and procedures from the Information Technology industry. We agree that we do not have a complete written policy and procedures manual for the Town's Information Technology Services. The Information Technology Department is in the process of creating, revising, and consolidating policies and procedures for the governance of Information Technology, including disaster recovery.

See Note 3 Page 10

We disagree with the audit findings that officials did not adequately safeguard online banking transactions, and the online banking agreement did not comply with GML. The Comptroller's Office established names and numbers of bank accounts authorized for electronic or wire transfers and individuals allowed to request electronic or wire transfer funds. The Comptroller's Office ensures that privileges and alerts are appropriate whenever establishing online bank accounts. We agree that there is no

See Note 4 Page 10

written online banking policy and a dedicated computer for online transactions. The Comptroller's office will create a written policy and procedure for online banking and a dedicated computer for online transactions.

Please contact me with any questions or concerns you may have about our operations.

Sincerely,

George J. Meyers
Town Supervisor

Appendix B: OSC Comments on the Town's Response

Note 1

We requested signed acknowledgement forms for 10 employees for the most recently adopted "Employee Handbook for Information Technology Security," adopted in September 2013. However, Town Officials provided us with signed acknowledgement forms pertaining to an outdated acceptable use policy that was adopted by the Board in 2005, nearly 15 years ago. Whenever the policy is updated it should be distributed to, read and acknowledged so employees are aware of the current policies.

Note 2

Town Officials did not provide us with documentation to substantiate their claims that employees received cybersecurity training.

Note 3

While Town officials' purport they have a disaster recovery plan and we asked for a copy of the plan; officials did not provide one.

Note 4

Although the Town had an online banking agreement, it did not contain all the requirements to comply with General Municipal Law which provide protections for Town funds.

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 reviewed Board minutes for resolutions concerning IT matters and reviewed Town policies to determine the number and scope of policies that were officially adopted.
- We interviewed officials and employees to obtain an understanding of the Town's IT operations.
- We reviewed Town records for any IT-related policies and procedures.
- We interviewed Town employees to determine what safeguards (if any) were in place to protect sensitive data and financial assets.
- We reviewed and evaluated eight[2] of the ten employees whose Internet use was assessed to determine compliance with the Town's acceptable use guidelines. We used our professional judgment to select employees based on job titles and responsibilities that involve accessing sensitive employee and financial PPSI.[3] We also interviewed these ten employees to determine whether they had received formal IT security awareness training.
- We ran a computerized audit script on the Town's domain controller.[4] We then analyzed the report, generated by the script, for inactive users. We also compared it to the employee master list to determine whether any network users were no longer employed by the Town.
- We ran a shared folders audit script on the Towns file directory server. We analyzed the report, generated by the script, to identify any folders that could potentially have contained files that indicated misuse of Town assets. We then determined who had access to those folders and verified the contents of the folders with officials.
- We asked officials whether the Town had a disaster recovery plan.
- We asked officials whether the Town had any written agreements with its banks. We also asked officials whether the Town had an online banking policy.

2 Using our judgment, we did not review the web history of two computers assigned to the police department as the websites accessed by officers may be required in the course of their duties. However, we did evaluate these devices to ensure software and patches were up-to-date and supported by the vendor.

3 These users had access to applications or systems containing PPSI, including online banking, payroll, human resources, student information and financial systems.

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

- We reviewed user access and permissions for the online banking application used by the Town and also determined whether there was proper segregation of duties and whether granted user permissions were necessary for each employee 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.

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

Appendix D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

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?title=&body_value=&field_topics_target_id=263206&issued=All

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/sites/default/files/local-government/documents/pdf/2020-05/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?title=&body_value=&field_topics_target_id=263211&issued=All

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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

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