REPORT OF EXAMINATION | 2019M-220

Town of Wappinger

Information Technology

MARCH 2020

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

Contents

Report Highlights

Town of Wappinger

Audit Objective

Determine whether Town officials ensured that the personal, private and sensitive information (PPSI) on Town servers was adequately protected from unauthorized access, use and loss.

Key Findings

- Town employees did not comply with and officials did not monitor the computer use policy.
- Twenty of 66 user accounts were not necessary for Town operations.
- Town officials did not develop a breach notification policy, disaster recovery plan or a policy addressing PPSI.

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

Key Recommendations

- Monitor web and computer usage for compliance with policy.
- Develop written procedures for managing system access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.
- Develop and adopt comprehensive IT policies that address breach notification, disaster recovery and PPSI, and communicate all adopted IT policies to Town officials, employees and the IT consultant.

Town officials generally agreed with our findings and indicated they plan to initiate corrective action.

Background

The Town of Wappinger (Town) is located in Dutchess County and contains the Village of Wappingers Falls. The Town is governed by a Town Board (Board) consisting of the Supervisor and four Council members, each representing a ward. All Board members are elected to two-year terms. The Supervisor is the presiding officer for the Town. The Board adopts resolutions, ordinances and local laws, and approves the annual budget and tax levy.

The Town contracts with an IT consultant (consultant) to perform IT-related services. The consultant is the network administrator and provides general IT support to all Town departments and employees. The consultant also makes recommendations to the Board regarding hardware and application acquisitions and/or changes. The Town has one main network containing all user accounts.

Quick Facts	
Network User Accounts	66
2019 General Fund Budgeted Appropriations	$4.7 million
Total Paid to Consultant (1/1/18-6/30/19)	$44,040

Audit Period

January 1, 2017 – July 9, 2019

We extended our audit period to September 9, 2019 to complete our IT testing.

Information Technology

How Should IT Systems Be Secured and Protected?

The Town's IT system and data are valuable resources. The Town relies on its IT system for Internet access, email, and for maintaining financial and personnel records. If the IT system is compromised, the results could be catastrophic and 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.

A town's governing body should establish computer policies that take into account people, processes and technology; communicate these policies throughout the town's departments; and ensure town officials develop procedures to monitor compliance with the policies. A computer use policy should be adopted that describes appropriate and inappropriate use of IT resources. Town officials should monitor compliance with that policy.

The Town's employee handbook includes a computer utilization policy that prohibits the use of the Town computer system for personal means. Further, the Town Code states that municipal resources should not be used for personal or private purposes. In addition, Town officials should require employees to sign acknowledgement forms to indicate they received the computer use policy to ensure employees are aware of and understand what is expected of them. Officials should also develop comprehensive written procedures for managing system access that include periodic reviews of user access to ensure that user accounts are disabled or deleted when access is no longer needed.

New York State Technology Law[1] requires municipalities to have a breach notification policy or local law that requires certain individuals to be notified when there is a system security breach involving private information. A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event that compromises the availability or integrity of an IT system and data. Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed 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. Additionally, such a plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

1 New York State Technology Law, Section 208

Town officials should develop and communicate written procedures for storing, classifying, accessing and disposing of personal, private or sensitive information (PPSI).[2] This policy should define PPSI; explain the entity's reasons for collecting PPSI; and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities.

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, Town officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data, and communicate related policies and procedures to all employees. The discussions could center on emerging trends in information theft and other social engineering[3] reminders; limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed; malicious software; virus protection; the dangers of downloading files and programs from the Internet; passwords; Wi-Fi security; and how to respond if a virus or an information security breach is detected.

Officials Did Not Monitor Compliance With the Computer Use Policy

While the Town has a computer use policy, it does not have a formal process to require employees to acknowledge they read the policy. Beginning in 2019, Town officials began requiring employees to sign acknowledgement forms indicating they read and understood Town policies. Previously, there was no requirement for employees to acknowledge the Town's computer use policy. We reviewed employee acknowledgement forms and found that 65 out of 105 employees (62 percent) did not acknowledge the computer use policy in the employee handbook. When policies are not clearly communicated, enforcement may be difficult. As a result of the policy not being communicated, employees may not understand the Town's expectation for use of Town computers.

We reviewed the website browsing histories of five[4] Town computers with access to PPSI and identified instances where employees accessed websites not related to Town business. Employees accessed websites related to social media, entertainment (including streaming websites), personal shopping, and personal investing and online banking. The consultant stated that while he periodically reviewed usage logs in the past, the server containing the logs failed in early 2019. As a result, Town officials do not have the ability to review web usage logs. The consultant stated that because the Town was planning to purchase a new

2 PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers (students), third parties or citizens of New York in general.

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

4 See sampling methodology in Appendix B.

firewall with web filtering and monitoring capabilities, it was not reasonable to replace the old server that stored the logs. When employees access websites for nonbusiness or inappropriate purposes, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections.

We also reviewed the programs installed on Town computers and found that one employee with access to PPSI installed programs for personal use such as personal tax preparation software and software relating to a navigational program. The consultant stated that some high-level employees are granted higher local access that allows the installation of programs. As a result, the employee could install programs for personal use. Personal software, even if for a governmental use, should not be installed on government computers because it would not have been tested on the network and could introduce viruses or other disruptions to the network. Software additions or changes should be made by IT administration, when practical, to ensure the software works well with the network, is safe to use, and is for business use.

Officials Did Not Develop Procedures for Managing System Access

Town officials have not developed comprehensive written procedures for managing system access for the Town's 66 user accounts. As a result, there is no formal process for notifying the consultant when an account should be removed from the Town's network. We examined the 66 user accounts on the Town's network and found 20 accounts that were not necessary for Town operations. Seven of these accounts belonged to former employees no longer with the Town; one of these accounts had not been used since August 2015. Thirteen of these accounts were generic accounts that were determined to not be needed. For example, the Town had created a generic account for auditors to use. However, the account has not been used since 2009 and is no longer used by the Town's auditors. Ten of the 13 generic accounts were never used. The consultant removed these identified accounts as we found them.

Town officials did not establish formal procedures for reviewing user accounts or disabling user accounts when employees separated from Town employment. As a result, there is nothing in place to inform the consultant when employees separate from Town employment. Having inactive user accounts that are not monitored increases the risk that these accounts could potentially be used by former employees or others for malicious purposes. Further, unnecessary accounts create additional work to manage network access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

The Board Did Not Adopt Adequate IT Security Policies

Breach Notification Policy – The Board and Town officials have not developed and adopted a written breach notification policy or local law because they were unaware of this requirement. As a result, if PPSI is compromised, officials may not fulfill the Town's legal obligation to notify affected individuals.

Disaster Recovery Plan – Town officials have not developed written procedures for disaster recovery and backup because they were unaware of this best practice. While the Town would contact the consultant in the event of a disaster, other employees should be aware of their roles and responsibilities in such an event. Furthermore, in the event of a disaster, Town officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data. Without a formal plan, the Town could lose important equipment, financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees. Given the prevalence of ransomware attacks on municipal computer systems, a disaster recovery plan is essential to protect IT assets.

Use of, Access to, and Storage and Disposal of PPSI – The Board and Town officials have not developed a classification scheme for PPSI or adopted a policy that identified the types of PPSI stored by the Town, where the PPSI should be located, and who should have access to it. The consultant stated that he was unaware of the data stored by the Town. Unless Town officials classify the data they maintain and set up appropriate security levels for PPSI, there is an increased risk that PPSI could be exposed to unauthorized users, and effort to properly notify affected parties in the event of a data breach could be hampered.

Officials Did Not Provide IT Security Awareness Training

Town officials did not provide users with IT security awareness training to help ensure they understand IT security measures designed to safeguard data from potential abuse or loss. The consultant stated that he provides informal training while he is on-site at the Town; however, Town employees have not been provided with comprehensive training.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. Town officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without 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, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT policies that address breach notification, disaster recovery and PPSI.

2. Require employees to read and verify understanding of the IT policies

Town officials should:

3. Monitor web and computer usage for compliance with policy and review installed software on a periodic basis.

4. Develop written procedures for managing system access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

5. Develop comprehensive IT policies that address breach notification; disaster recovery plan including backup procedures; and classification of, use of, access to and storage and disposal of PPSI, and communicate all adopted IT policies to Town officials, employees and the consultant.[5]

6. Develop a comprehensive disaster recovery plan, and update and test the plan periodically.

7. Ensure that IT security awareness training is provided periodically to all employees who use computers.

5 Refer to our publication Information Technology Governance available at www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

Appendix A: Response From Town Officials

SUPERVISOR
Dr. Richard L. Thurston

Confidential Secretary
Sandra Vacchio

20 MIDDLEBUSH ROAD
WAPPINGERS FALLS, NY 12590

WWW.TOWNOFWAPPINGERNY.GOV
(845) 297-4158 - Main
(845) 297-2744 - Direct
(845) 297-4558 – Fax

TOWN OF WAPPINGER

Office of the Town Supervisor

TOWN BOARD
William H. Beale
Angela Bettina
Chris Phillips
Alfred Casella

TOWN CLERK
Joseph P. Paoloni

HIGHWAY SUPERINTENDENT
Michael Sheehan

February 28, 2020

We have reviewed the findings of the IT security audit report. Since the current Thurston Administration took over the Supervisor's Office in January 2018, the Town government has focused on continuous improvement of what had been found to be an antiquated IT system. Therefore, overall, the report's findings accurately reflect the remaining issues that had not yet been addressed prior to the audit.

Additional improvements have been made to address the potential vulnerabilities, including:

1. We have implemented a number of computer and IT usage policies and controls throughout our offices.

2. We have been and will be conducting regular audits of our computers and IT systems throughout all departments, and have not found any new unauthorized and unsupported software.

3. The audit revealed 20 user accounts in the active directory that were not necessary for Town operations. We have removed all of these accounts. Many of those accounts were for former employees, and some of them were created for software vendors for the purpose of assigning restricted permission to a particular software solution for remote support purposes.

4. The Town has ensured that any separation from a Town employee will be communicated properly to the appointed IT consultant, so that any existing user accounts can be disabled and/or removed at the time of separation. Furthermore, accounts established for software vendors will be reviewed quarterly, and any account deemed unnecessary will be disabled.

5. The Town has purchased and deployed new, robust firewall security appliances. The appliances include modern security features that greatly improve the security and prevention capabilities of cyber threats. One of the key recommendations in the audit report is to monitor web usage for compliance with the Town's computer use policy. *Even before the recommendations were provided*, the Town had already planned on the deployment of a web content filtering policy. This policy was configured and deployed immediately at the time of installation of the new security appliance. Any category of content that is not pertinent to Town business (pornography, online dating, online gaming, etc.) is blocked.

6. Any internal/employee attempt to access a website with prohibited content is logged. And, the Town is in the process of procuring a solution with the ability to produce reports of web activity for any or all users and Town computers. However, some categories, such as social networking, are gray areas. There are select staff members that manage the Town's social media accounts, pursuant to the Town's *Social Media Policy.* This use of Social Media by authorized Town personnel makes the notion of blocking social networking sites infeasible. The use of social networking is governed by the adopted *Social Media Policy*. Any other category of content that falls in a gray area will be handled in a similar fashion.

7. The Town is currently developing a comprehensive business continuity policy and plan which will have a number of elements, including:

    a. Town data is backed up and stored both locally and off-site, and the data is protected from potential geographical disaster. Additionally, we are in the process of exploring and researching options to provide

immediate access to Town systems in the form of an off-site or cloud operations center.

b. Certain PPSI information is not listed in our IT systems while some information does exist. Accordingly, we are now conducting an audit of the nature and locations of all information that may be considered to fall within the PPSI category; and

c. The Town's ultimate goal is to have the ability to carry-on any IT operations should the Town Hall be affected by an unforeseen disaster. As part of this objective, the Board will be reviewing and approving a comprehensive Continuity Plan and IT Policy shortly. These new, to-be-adopted policies will be in addition to the existing computer utilization policy that exists in the current employee handbook.

Once the new policies, plans and procedures are soon in place, the Town will periodically provide to all employees and consultants IT security awareness training that explains the policies and instructs on the proper rules of behavior for using the internet, the Town's IT systems, its Social Media Policy as well as how best to secure PPSI information. All employees and consultants will be required to attend these training sessions as well as to continue to acknowledge familiarity of such policies and procedures. All new employees will sign such an acknowledgement as well as attend a training program.

Sincerely,

Richard Thurston, 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 reviewed the Town's Code and Employee Handbook to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We reviewed a listing provided by the Town that indicated which employees had signed acknowledgements that they had read the Employee Handbook. The listing indicated that 40 employees had signed acknowledgements. We tested a random sample of five employees to obtain reasonable assurance that the list was accurate.
- We interviewed officials and personnel to gain an understanding of internal controls over IT.
- We used our professional judgment to select a sample of five out of the 46 Town computers. We selected the sample of five users who had access to PPSI.[6] We reviewed web history reports from these computers for accessed websites that could put the network at risk.[7] We ran an audit script on each computer that retrieved installed software. We reviewed the software for indications of personal use.
- We ran a computerized audit script to analyze Town folders. We used the script output to identify any folders that could potentially contain files that indicated misuse of Town computers. We then determined who had access to those folders and verified the contents of the folders with Town officials.
- We ran a computerized audit script to analyze the Town's network information about users to determine whether users' accounts were necessary. We reviewed user accounts and compared them to a list of current employees to identify potentially inactive and unnecessary accounts. We interviewed Town officials to determine the necessity of the identified accounts.
- We inquired about a breach notification policy, disaster recovery plan and backup procedures.

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.

6 These users had access to key financial applications and related PPSI including payroll and human resources.

7 One of the five computers tested produced no web history.

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

Appendix C: Resources and Services

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

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

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

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

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

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

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

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

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

Contact

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

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

www.osc.state.ny.us/localgov/index.htm

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

NEWBURGH REGIONAL OFFICE – Lisa 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