REPORT OF EXAMINATION | 2020M-153

Town of Fishkill

Information Technology

APRIL 2021

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

Contents

Report Highlights

Town of Fishkill

Audit Objective

Determine whether Town of Fishkill (Town) officials ensured the Town's Information Technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

Town officials did not adequately secure and protect the Town's IT systems against unauthorized use, access and loss.

- The Board did not adopt adequate IT policies or a disaster recovery plan.
- Officials did not adequately manage user accounts for the network or financial application.
- Town employees did not comply with the acceptable use policy (AUP) and officials did not monitor the use of IT resources.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies and a disaster recovery plan.
- Develop written procedures for managing system access.

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

Background

The Town is located in the southwest part of Dutchess County. The Town is governed by an elected Town Board (Board) composed of four Board members and the Town Supervisor (Supervisor). The Board is responsible for managing operations.

The Town's planning board secretary is the network administrator (Administrator). The Town contracts with an IT consultant to perform IT-related services. Together they provide general IT support to all departments and employees.

The Supervisor, in consultation with the Administrator and IT consultant makes recommendations to the Board regarding hardware and application acquisitions and/or changes.

Quick Facts	
Servers	1
Computers	42
Employees	145
Total Paid to IT Consultant	$16,500

Audit Period

January 1, 2019 – February 29, 2020

Information Technology

The Town's IT system and data are valuable resources. The Town relies on its IT assets for Internet access, email and maintaining financial and personnel records, much of which contain personal, private and sensitive information (PPSI). PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general.

When an 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.

How Should IT Systems Be Secured and Protected?

IT policies such as password, wireless security and mobile and removable device describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board should establish security policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

Officials should develop and communicate a written policy and procedures for storing, classifying, accessing and disposing of PPSI. 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. Officials should also inventory PPSI by classifying all Town data, and identifying where it is stored in the computer system and who uses it. Officials should periodically review and update the inventory.

A disaster recovery plan typically includes an analysis of business processes and continuity needs, disaster 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.

The Board Did Not Adopt Adequate IT Policies

IT Policies –Town officials did not develop and the Board did not adopt password, wireless security and mobile and removable device policies. A lack of appropriate policies significantly increases the risk that data, hardware and software systems

may be lost or damaged by inappropriate access and use. Without properly designed and functioning controls there is a likelihood that significant errors or fraud will occur and remain undetected.

Use of, Access to and Storage and Disposal of PPSI –Town officials have not developed a written policy that defines PPSI, explains the reason for collecting PPSI, nor written procedures for use, access to, storage and disposal of PPSI. Furthermore, officials have not established a data classification scheme or conducted an inventory of PPSI. Unless 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.

Disaster Recovery Plan – The Board did not develop a disaster recovery plan. This plan documents how Town officials would respond to potential disasters. Consequently, in the event of a disaster or a phishing[1] or ransomware attack, staff had no guidance or plan to follow to restore or resume essential operations in a timely manner. Officials told us that they are in the process of developing a disaster recovery plan. Without a formal written plan, the Town has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

The Board did not adopt a disaster recovery plan.

Backup Procedures – The Administrator does regular back-ups for the Town at an off-site location and through the cloud. Cloud-based storage makes it possible to save files to a remote location and retrieve them on demand. However, Town officials have not developed written procedures describing their backup process. Although the Administrator told us that back-ups are performed periodically, we did not find any evidence or documentation that officials attempted to restore a backup to ensure the process is functioning as intended and that data would be available in the event of an emergency. Without formal written backup procedures, the Town has an increased risk that it could not restore operations quickly and effectively following a service disruption.

Why Should the Town Manage User Accounts?

User accounts provide access to networks and financial applications and should be actively managed to minimize the risk of unauthorized access or misuse. A town should have written procedures for granting, changing and revoking access rights to the network and financial application.

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

In addition, town officials should regularly review enabled network user accounts to ensure they are still needed. Officials must disable unnecessary or unneeded accounts as soon as there is no longer a need for them, including user accounts of former employees or employees who have transferred to another area. The Administrator is responsible to ensure user accounts are managed appropriately.

Officials should segregate duties within the financial application to ensure that employees are granted access needed to perform their duties but cannot perform all phases of a transaction. Additionally, audit logs should be reviewed to ensure individuals are making only authorized changes in the application. Any unusual or unauthorized activity could indicate a breakdown in controls or possible malfeasance.

Effective controls over access rights to the financial application should allow users access to those computerized functions that are consistent with their job responsibilities and should prevent users from being involved in multiple aspects of financial transactions. The written procedures should establish who has the authority to grant or change access and allow users to access only what is necessary to complete their job duties.

Town Officials Did Not Adequately Manage User Accounts

Town officials did not establish procedures to manage user accounts for its network and financial application, or maintain a list of authorized users and their level of access. In addition, officials did not review audit logs to ensure individuals are making only authorized changes.

[W]e found unneeded accounts that had not been disabled…

As a result, we found unneeded accounts that had not been disabled and/or monitored, and some Town employees with access to the financial application had excessive user permissions and access to employees' PPSI, as follows:

Employees – For both the network and financial application, when employees are hired or leave employment, officials notify the Administrator of the level of access needed or needed to be removed either verbally or in writing depending on the department.

Due to the lack of written procedures, we reviewed all 87 network accounts and found 13 former employees with enabled network accounts. The Administrator told us she only enables or disables accounts when she is notified by a department head. User accounts of former employees that have not been disabled or removed could be used by those individuals or others for malicious purposes.

Unneeded Generic Accounts – Of the 87 network accounts reviewed, we also found 13 generic accounts that were no longer needed. After we notified the Administrator of the existence of the unneeded accounts, she told us that she

subsequently disabled these accounts. Unnecessary accounts must be disabled as soon as there is no longer a need for them.

Financial Application User Permissions – We reviewed the 21 permissions for the Town's financial application. We found 13 former employees who had active user accounts and seven users with excessive permissions not consistent with their former or current job responsibilities. These excessive permissions provided the users with the ability to control multiple aspects of a financial transaction and access to unnecessary PPSI. The following users had excessive permissions:

- The Administrator had access to accounts payable, budgeting, general ledger, purchase orders, human resources, payroll and accounts receivable, but does not have any financial job duties.
- The senior accountant had access to delete and/or modify purchase orders after they are paid, and is a human resources super user (system administrator), but does not have those job duties.
- The accounts payable clerk had access to human resources, accounts receivable, journal entries, budgeting, utility billing and general ledger, and is a payroll super user, but does not have those job duties.
- The purchasing agent had access to accounts receivable, accounts payable, general ledger, system administration, and is a utility billing super user, but does not have those job duties.
- One clerk had access to human resources, payroll, utility billing, system administration workflow super user, budgeting and journal entries, but does not have those job duties.
- Two clerks had access to accounts payable and general ledger, but do not have those job duties.
- The accounts payable clerk had access to social security numbers and dates of birth, but did not need to have that access for their job duties.

[T]here is an increased risk…to the financial application…

The Comptroller told us that she was unaware that users had excessive user permissions to the financial application and that the Town has not stored payroll or human resource data in their financial system for the past two years; however, there is historical data saved in the application. As a result, there is risk of exposure of PPSI and there is an increased risk that intentional or unintentional changes to the financial application could occur without detection.

Having unnecessary permissions within the network and financial application could result in an abuse of those permissions either by the user or by a malicious outsider that had obtained that user's credentials. Abuse of these permissions could include monetary theft, fraud, attempts to cover up fraud, identity theft and other criminal activities. Additionally, users with these excessive permissions

may be unnecessarily subject to investigation if instances of wrongdoing are discovered within the system.

How Should Officials Monitor and Enforce the AUP?

A town should have a written AUP that defines the procedures for computer, Internet and email use and describes what constitutes appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP.

Monitoring compliance with AUPs involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, AUP or standard security practices.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. Town officials can reduce the risks to PPSI and IT assets by routinely monitoring Internet usage and developing and implementing procedures to ensure employee compliance with the AUP. In addition, such activity may interfere with an employee's job performance or productivity, lead to inadvertent information disclosure or, when online banking is involved, theft of Town funds.

Town Officials Did Not Enforce the AUP

The Town has a comprehensive AUP that defines the procedures for computer, Internet and email use. The policy describes what constitutes appropriate and inappropriate use of IT resources and states that employees are responsible for exercising good judgement regarding reasonableness of personal use. Any non-business use should be incidental and occasional.

We reviewed the web browsing history on five[2] computers and found questionable Internet use on one computer from the previous Town Supervisor. To determine reasonableness of personal use, we reviewed internet usage that exceeded 30 minutes[3] of personal use in a single day. We found there were nine days of personal internet usage that exceeded 30 minutes out of 303 days from March 4, 2019 to December 31, 2019. This included social media use, campaigning, personal shopping, online banking, real estate searches, maps, accessing

2 Refer to Appendix B for information on our sampling methodology

3 Using our professional judgement, we determined that personal use exceeding 30 minutes was not reasonable.

entertainment websites (including streaming) and web search browsing for non-Town related subjects. Because Town officials did not monitor employee Internet use, they were unaware of this personal and inappropriate computer use.

Inappropriate Internet activity may lead to inadvertent information disclosure or, introduce viruses, ransomware and other types of malicious software into the Town's computing environment. The malicious software could compromise PPSI and Town computers, and any PPSI contained has a higher risk of exposure to damage and PPSI breach, loss or misuse.

Inappropriate Internet activity may lead to inadvertent information disclosure…

What Do We Recommend?

The Board Should:

1. Adopt comprehensive IT policies to address passwords, wireless security, mobile and removable devices and data backup, and communicate the policies to Town officials, employees and the IT consultant.[4]
2. Develop a PPSI policy, inventory PPSI and periodically review and update the inventory.
3. Develop a comprehensive disaster recovery plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure it works as intended.

Town Officials should:

4. Develop written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed for the network or financial application.
5. Periodically review financial application access and limit access to ensure authorizing, transmitting, recording and approving transactions are segregated and that access is based on job function.
6. Periodically review audit logs to make sure employees are making only authorized entries in the financial accounting system.
7. Design and implement procedures to monitor the use of IT resources, including personal use, for compliance with the Town's AUP.

4 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

Ozzy Albra, Town Supervisor
E-mail: supervisor@fishkill-ny.gov
(845) 831-7800 Ext. 3309
(845) 831-6040 Fax

Fishkill Town Hall
807 Route 52
Fishkill, NY 12524-3110
website: www.fishkill-ny.gov

March 16, 2021

Honorable Thomas P. DiNapoli, Comptroller
New York State
110 State St.
Albany, NY, 12207

Dear Comptroller DiNapoli,

I would like to begin by thanking you for granting my request to come into the Town of Fishkill and perform an audit. When I took office in January of 2020, I requested this audit to obtain a clear picture of the strengths and weaknesses of the Town's IT systems, procedures and policies. In keeping with my well-known commitment to efficient and transparent government, I wanted to establish which policies already in place in the Town were effective, and which need further development and improvement.

The Town is in receipt of the Audit Report compiled by your office, and has reviewed all of your recommendations. After careful review of the comprehensive report, the Town of Fishkill is in agreement with the findings and guidance contained in the audit report.

Since the audit began, the Town has begun the process of developing detailed written policies to address the deficiencies found during the audit. These policies will give greater authority to the Network Administrator for enforcement purposes. These policies and procedures, when completed and put in place, will enable the Town to address the concerns enumerated in the report, and ensure the successful operation of Town IT systems moving forward at the highest possible levels of security.

As a result of the audit, the Town has taken some immediate corrective actions:

- Removed users and denied their access for terminated employees.
- Removed senior accountant access to delete or modify purchase orders.
- Removed software from Town desktops and laptops that is not required for Town business.
- Restricted internet browsing to certain websites to limit personal internet usage and reduce risk of viruses, ransomware and other malicious software.

Thank you again for responding to my request for an audit. Based on the findings contained in the audit report, my administration will take swift and decisive action to implement measures which will improve the Town's IT systems and security for years to come.

Regards,

Azem "Ozzy" Albra
Town Supervisor
Town of Fishkill

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 Employee Handbook to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We reviewed a list provided by the Town that indicated which employees had signed acknowledgements that they had read the Employee Handbook. We selected a random sample of five out of 145 active employees to obtain reasonable assurance that the list was accurate.
- We inquired about a breach notification policy, PPSI policy, disaster recovery plan and backup procedures to determine whether these policies, plans and procedures were adopted and working as intended.
- We interviewed officials and personnel to gain an understanding of the IT environment and internal controls over IT assets.
- We ran a computerized audit script on the Town's domain controller.[5] We then analyzed the report to determine if all users were currently employed by the Town.
- We reviewed user access rights for the Town's financial application and evaluated permissions to determine whether user access is properly segregated and based on job function.
- We reviewed the Town's audit log to determine if anyone accessed PPSI.
- We used our professional judgment to select five of the 47 computers used by employees who had access to PPSI[6] and reviewed their web history reports. We evaluated the reports to determine whether internet use was in compliance with the AUP guidelines.

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

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

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

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/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