DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-164

City of Peekskill

Information Technology

APRIL 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

City of Peekskill

Audit Objective

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

Key Findings

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

- Adequate IT policies and a disaster recovery plan were not developed or adopted.
- Internet usage was not monitored and the Acceptable Use Policy (AUP) which describes what constitutes appropriate and inappropriate use of IT resources was not enforced.
- Network User Accounts were not adequately managed.
- IT security awareness training was not provided.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies and a disaster recovery plan.
- Provide periodic IT security awareness training to all employees who use IT resources.

District officials generally agreed with our recommendations and indicated they plan to initiate corrective action.

Background

The City is located in Westchester County. An elected seven-member City Council (Council) is responsible for providing oversight of City operations.

The City Manager serves as the City's chief executive officer and is responsible, along with other administrative staff, for the City's day-to-day administration.

City officials contracted with a third-party consultant (IT consultant) to manage the City's IT systems. The City also employs an in-house IT support technician who handles the day-to-day computer related issues.

Quick Facts	
Enabled Network accounts	309
Computers	100
2020 Budgeted Expenditure IT Contractor	$142,500
Employees	221

Audit Period

January 1, 2018 – October 15, 2019. We extended our scope forward to March 12, 2020 to complete computer testing.

Information Technology

How Do Policies Secure and Protect City IT Systems?

A city relies on its IT assets for Internet access, email and for maintenance of financial, personnel and taxpayer records, much of which contain personal, private and sensitive information (PPSI).[1] If the IT system is compromised, the results could range from inconvenient to catastrophic and may 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.

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A council 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.

A council 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.

New York State Technology Law[2] requires municipalities to adopt a breach notification policy or local law that details actions to be taken to notify affected individuals when there is a system security breach involving personal information. In addition, IT security policies should address data classification and regulations that ensure officials identify and organize city data to determine what data exists, where it is located and how to protect it.[3]

Because different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored. In some instances, laws, regulations or a city's policies predefine the classification of each data type. To minimize the risk of data loss or suffering a serious interruption of services, city officials should establish a formal written disaster recovery plan.

This is particularly important given the current and growing threat of phishing and ransomware attacks.[4] 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 financial system and any PPSI contained therein.

[1] 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.

[2] New York State Technology Law, Section 208

[3] Data classification is the process of assigning data to a category that will help determine the level of internal controls over that data.

[4] Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software. Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made.

Typically, a disaster recovery plan involves analyzing business processes and continuity needs, assuming that all relevant disasters will occur and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. Additionally, 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 Council Did Not Adopt Adequate IT Security Policies

Breach Notification Policy – The Council has not developed and adopted a breach notification policy or local law because it was unaware of this requirement. As a result, if PPSI is compromised, officials may not be able to fulfill the City's legal obligation to notify affected individuals to inform them of the need to monitor credit reports and bank activity.

Use of, Access to, and Storage and Disposal of PPSI – The Council has not adopted a policy that identifies the types of PPSI stored, explains the reason for collecting PPSI or specific procedures for use, access to, and storage and disposal of PPSI involved in normal business activities. Furthermore, officials have not developed a data classification system for PPSI. The consultant stated that he was unaware of the data stored by the City. 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 efforts to properly notify affected parties in the event of a data breach could be hampered.

…[I]f PPSI is compromised, officials may not be able to fulfill the City's legal obligation to notify affected individuals…

Disaster Recovery Plan – City officials performed data backups, which were encrypted, stored offsite and periodically tested. However, the Council did not develop a disaster recovery plan to address potential disasters. Therefore, in the event of a disaster or a phishing or ransomware attack, officials have no guidance or plan to follow to minimize or prevent the loss of equipment or data. While City officials would contact the consultant in the event of a disaster, other employees should be aware of their roles and responsibilities in such an event.

City officials told us that they were unaware they should develop a disaster recovery plan. Without a formal plan, the City could lose important equipment, financial and other data and suffer a serious interruption to operations, such as not being able to process payments to vendors or employees.

While policies alone will not guarantee the safety of IT assets and data, a lack of appropriate policies significantly increases the risk that data, hardware and software may be lost or damaged by unintentional or inappropriate use or access.

How Should Officials Monitor and Enforce the Acceptable Use Policy?

A city should have an AUP that defines the procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment, user privacy and consequences for violating the AUP. In addition, officials should require employees sign acknowledgement forms to indicate they had read the city's AUP, were aware of what was expected of them and acknowledge they would be held accountable to the policies and procedures outlined in the AUP.

Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity and investigating and reporting indications of inappropriate or unusual activity. Officials should monitor and analyze activities for signs of possible or imminent threats of violations of computer security policies, acceptable use policies or standard security practices. Automated mechanisms may be used to perform this process, helping security professionals routinely assess computer security, perform incident investigations and even recognize an ongoing attempt of unauthorized access.

Internet browsing increases the likelihood users will be exposed to malicious software that may compromise data confidentiality, integrity or availability. City officials can reduce the risks to PPSI and IT assets by routinely monitoring Internet use and developing and implementing procedures to ensure employee compliance with the AUP. Officials should also ensure a city's network is used for appropriate purposes and an adequate web filtering process is in place to limit vulnerabilities in its IT systems through Internet browsing. 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 city funds.

Officials Did Not Enforce the AUP

The City has an AUP that defines the procedures for computer, Internet and email use as part of its employee handbook. The policy describes what constitutes appropriate and inappropriate use of IT resources and the City's expectations concerning personal use of IT equipment and user privacy. Further, the policy prohibits use of the City's computer system for personal purposes.

City officials did not monitor employee Internet use or implement procedures to monitor for compliance with the City's AUP. In addition, although employees are required to sign an acknowledgment form indicating they had read and understood the AUP, officials could not provide any evidence the employees signed these forms. Because officials did not ensure employees signed or otherwise acknowledged they had read and understood the AUP, there was an increased risk of exposing the City's IT systems and data to loss or misuse.

We reviewed the web browsing history of 10 computers assigned to 10 employees and found personal and inappropriate Internet use on two computers. This included online shopping, travel and social networking sites. The employees using these computers performed job duties that routinely involved accessing PPSI.

City officials told us they did not have tools to monitor Internet use. Because City officials did not monitor employee Internet use, they were unaware of this personal and inappropriate computer use. In addition, the web filter was not set to block websites that are frequently used for high risk personal purposes.

The City's failure to monitor Internet use increases the risk of improper use by employees and puts the IT system at risk, potentially resulting in the manipulation, destruction or theft of valuable City data. Because Internet browsing increases the likelihood of the City's computer system being exposed to malicious software that may compromise PPSI, City computers containing PPSI have a higher risk of exposure to damage and PPSI breach, loss or misuse.

Why Should City Officials Properly Manage User Accounts?

User accounts provide access to a city's network and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers to inappropriately access and view PPSI on the network. A city should have written procedures for granting, changing and revoking user permissions to the network.

In addition, to minimize the risk of unauthorized access, city officials should regularly review enabled network user accounts to ensure they are still needed. Officials must disable unnecessary or unneeded accounts promptly, including user accounts of former employees.

Officials Did Not Adequately Manage User Accounts

City officials did not develop comprehensive written policies and procedures for managing system access and did not adequately manage user accounts for the City's network. Although the IT consultant and IT support employee were responsible for ensuring user accounts for the IT system were managed in a timely and satisfactory manner, we found unnecessary user accounts that were not disabled.

We reviewed all of the City's 309 network accounts and found that 30 accounts belonged to former employees. One of these former employees had left City employment in August 2003. Officials told us these accounts were not disabled because a notification to request deactivation was not sent to the IT technical support employee upon each employee's separation.

Without formal procedures for regularly reviewing enabled user accounts, the City had a greater risk that the unneeded accounts could be compromised or used for malicious purposes. Unneeded network accounts must be disabled promptly to decrease the risk of unauthorized access and potential entry points for attackers to access PPSI.

Why Should City Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, city officials should provide periodic IT security awareness training. The training should explain policies and procedures to all employees and communicate the proper rules of behavior for using the Internet and IT systems and data.

The training should center on emerging trends which may result in PPSI compromise or denying access to the IT system and its data. This includes computer viruses and other types of malicious software, information theft and social engineering attacks.[5] Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of 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.

We interviewed three employees and found that none had received or were offered IT security awareness training.

Officials Did Not Provide IT Security Awareness Training

City 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. We interviewed three employees and found that none had received or were offered IT security awareness training.

Officials told us that they assumed employees were sufficiently aware of the City's security policies and were unaware of the need for IT security training.

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, the City could be at greater risk for unauthorized access and misuse or loss of data and PPSI.

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

The cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. City officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that employees understand the IT security policies and procedures and their roles and responsibilities related to IT and data security.

What Do We Recommend?

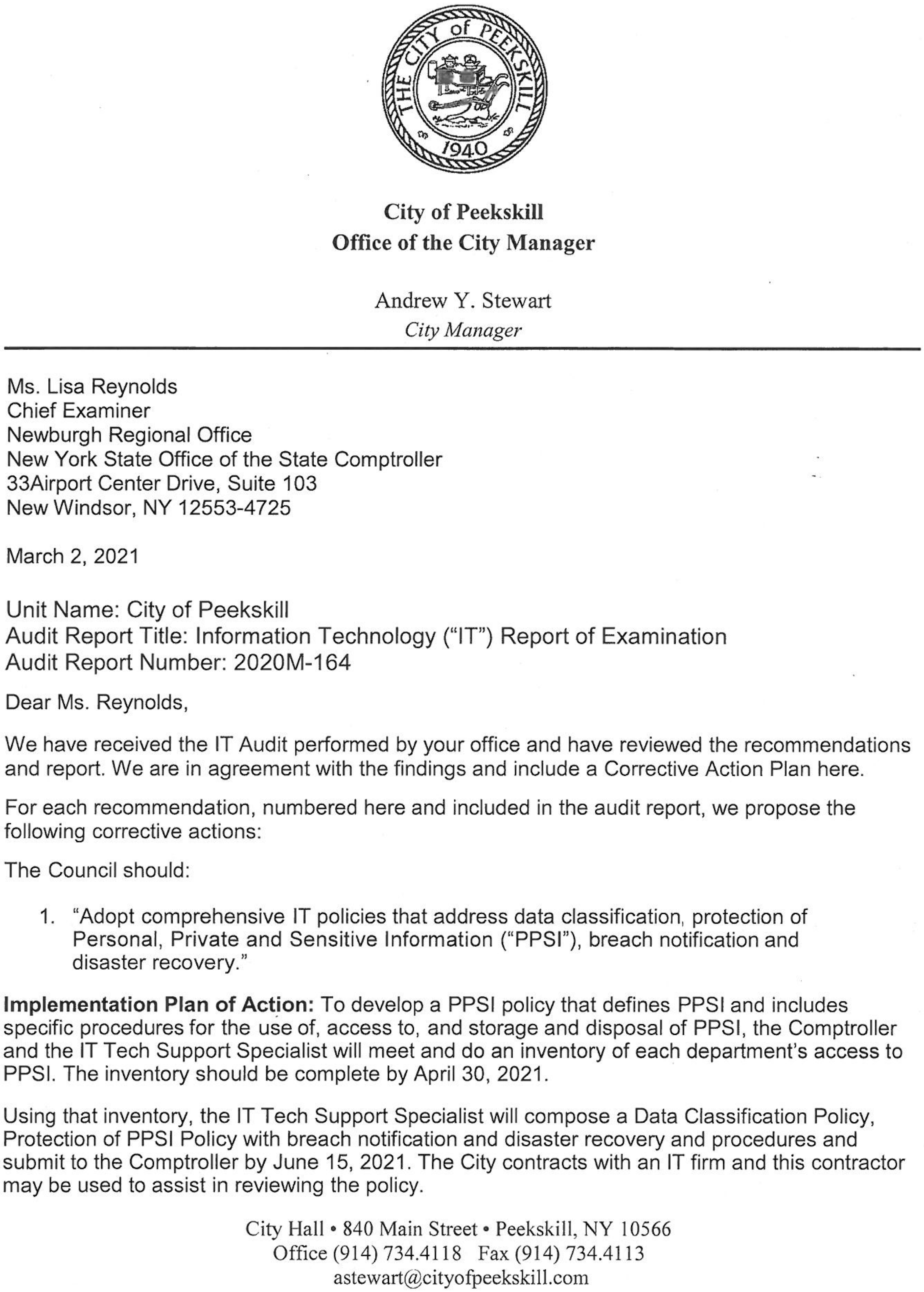
The Council should:

1. Adopt comprehensive IT policies that address data classification, protection of PPSI, breach notification and disaster recovery.
2. Require employees to read and verify their understanding of the IT policies.

City officials should:

3. Develop a comprehensive, written disaster recovery plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure it works as intended.
4. Ensure that all network users sign an acknowledgement as evidence that they read, were aware of and acknowledged they would be held accountable for compliance with the AUP.
5. Design and implement procedures to monitor employees' computer use and implement procedures to ensure compliance with the policy.
6. Configure the web filtering software to block sites that violate the AUP.
7. Develop written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed.
8. Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use and reflects current risks identified by the IT community.

Appendix A: Response From City Officials



City of Peekskill
Office of the City Manager

Andrew Y. Stewart
City Manager

Ms. Lisa Reynolds
Chief Examiner
Newburgh Regional Office
New York State Office of the State Comptroller
33Airport Center Drive, Suite 103
New Windsor, NY 12553-4725

March 2, 2021

Unit Name: City of Peekskill
Audit Report Title: Information Technology ("IT") Report of Examination
Audit Report Number: 2020M-164

Dear Ms. Reynolds,

We have received the IT Audit performed by your office and have reviewed the recommendations and report. We are in agreement with the findings and include a Corrective Action Plan here.

For each recommendation, numbered here and included in the audit report, we propose the following corrective actions:

The Council should:

1. "Adopt comprehensive IT policies that address data classification, protection of Personal, Private and Sensitive Information ("PPSI"), breach notification and disaster recovery."

Implementation Plan of Action: To develop a PPSI policy that defines PPSI and includes specific procedures for the use of, access to, and storage and disposal of PPSI, the Comptroller and the IT Tech Support Specialist will meet and do an inventory of each department's access to PPSI. The inventory should be complete by April 30, 2021.

Using that inventory, the IT Tech Support Specialist will compose a Data Classification Policy, Protection of PPSI Policy with breach notification and disaster recovery and procedures and submit to the Comptroller by June 15, 2021. The City contracts with an IT firm and this contractor may be used to assist in reviewing the policy.

City Hall • 840 Main Street • Peekskill, NY 10566
Office (914) 734.4118   Fax (914) 734.4113
astewart@cityofpeekskill.com

The Comptroller will present a draft to the City Manager for review by July 15, 2021.

A draft policy will then be presented to the City Council to be passed as a resolution, no later than August 31, 2021.

Implementation Date: A first draft will be presented to the City Manager by April 30, 2021 and a final draft resolution will be presented to the City Council by June 15, 2021 with a resolution to be approved no later than August 31, 2021.

Person Responsible for Implementation: Comptroller

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

Implementation Plan of Action: The Comptroller will email all employees, with IT access, who should be reading the Policies and they will be given an acknowledgement receipt to sign and return to the Comptroller. The signed receipts will be kept and maintained in the Human Resources Department's employee files.

Implementation Date: The email will be sent by September 30, 2021 and employees will be requested to return signed acknowledgements no later than October 31, 2021.

Person Responsible for Implementation: Comptroller

The Audit Report states that Management should:

3. "Develop a comprehensive, written disaster recovery plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure it works as intended.'

Implementation Plan of Action: To develop a disaster recovery plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure it works as intended, the Comptroller and the IT Tech Support Specialist will meet and do an inventory of each department's potential disasters. The inventory should be complete by May 31, 2021.

Using that inventory, the IT Tech Support Specialist will compose a Data Classification Policy, Protection of PPSI Policy with breach notification and disaster recovery and procedures and submit to the Comptroller by June 15, 2021. The IT contractor may be used to assist in reviewing the policy.

The Comptroller will present a draft to the City Manager for review by August 15, 2021.

A draft policy will then be presented to the City Council to be passed as a resolution, no later than September 30, 2021.

Implementation Date: A first draft resolution of the disaster recovery plan will be adopted by the City Council no later than October 31, 2021.

Person Responsible for Implementation: Comptroller

4. "Ensure that all network users sign an acknowledgement as evidence that they read, were aware of and acknowledged they would be held accountable for compliance with the AUP."

Implementation Plan of Action: The Comptroller will email all employees, with IT access, who should be reading the Policies and they will be given an acknowledgement receipt to sign and return to the Comptroller. The signed receipts will be kept and maintained in the Human Resources Department's employee files.

Implementation Date: The email will be sent by September 30, 2021 and employees will be requested to return signed acknowledgements no later than October 31, 2021.

Person Responsible for Implementation: Comptroller

5. "Design and implement procedures to monitor employees' computer use and implement procedures to ensure compliance with the policy."

Implementation Plan of Action: The IT Tech Support Specialist will design procedures to monitor employees' computer use as well as procedures to ensure compliance with the policy. Comptroller will review the procedures and present the procedures to the City Manager for his review. Comptroller will email all employees, with IT access, who will be notified that their computer use will be monitored.

Implementation Date: The procedures will be written and adopted by August 31, 2021.

Person Responsible for Implementation: Comptroller

6. "Configure the web filtering software to block sites that violate the Acceptable Use Policy ("AUP")."

Implementation Plan of Action: IT Tech Support Specialist will configure web filtering software to block sites that violate the AUP. The City's IT contractor might be utilized if necessary.

Implementation Date: Web filtering software will be configured by September 30, 2021.

Person Responsible for Implementation: IT Tech Support Specialist

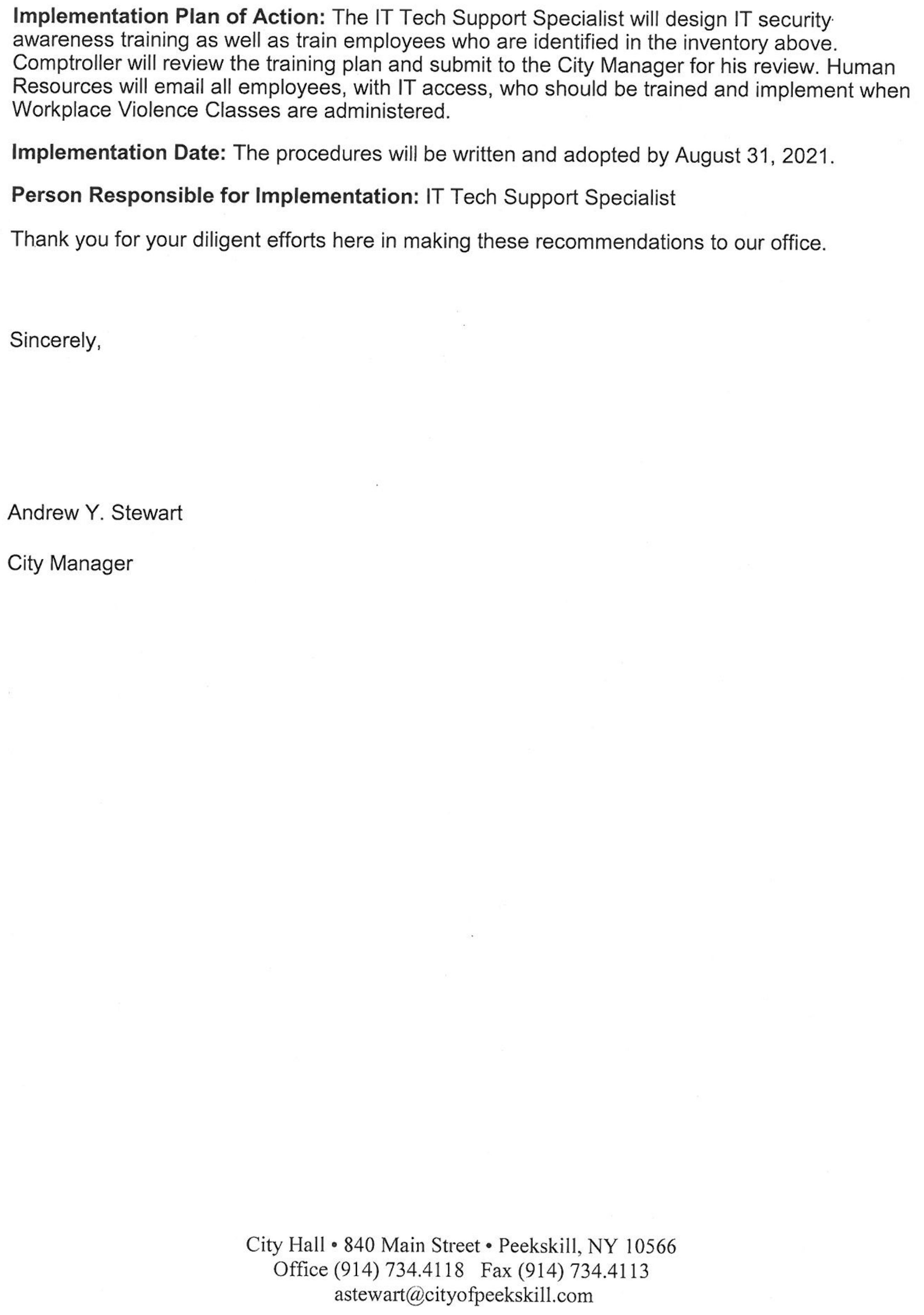
7. "Develop written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed."

Implementation Plan of Action: The IT Tech Support Specialist will design procedures to manage system access that include periodically reviewing user access and disabling user accounts when access is no longer needed.

Implementation Date: The procedures will be written and adopted by August 31, 2021.

Person Responsible for Implementation: IT Tech Support Specialist

8. "Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use and reflects current risks identified by the IT community."



Implementation Plan of Action: The IT Tech Support Specialist will design IT security awareness training as well as train employees who are identified in the inventory above. Comptroller will review the training plan and submit to the City Manager for his review. Human Resources will email all employees, with IT access, who should be trained and implement when Workplace Violence Classes are administered.

Implementation Date: The procedures will be written and adopted by August 31, 2021.

Person Responsible for Implementation: IT Tech Support Specialist

Thank you for your diligent efforts here in making these recommendations to our office.

Sincerely,

Andrew Y. Stewart

City Manager

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 Council minutes for resolutions and City codes concerning IT matters.
- We reviewed the employee handbook and other City records for any IT-related policies and procedures.
- We interviewed officials and employees to obtain an understanding of City IT operations and employee training.
- We interviewed City employees to determine whether any safeguards were in place to protect sensitive data and financial assets.
- We reviewed 10 employees' Internet use on the 10 computers assigned to them to evaluate whether their Internet use was in compliance with the City's AUP. We used our professional judgment to select these employees based on job duties that involve accessing PPSI.
- We ran a computerized audit script on the City's domain controller.[6] We compared the report generated by the script to the active employee master list to determine whether any network users were no longer employed by the City. We updated the testing to properly account for the seven elected officials that are not included on the active employee list as they do not receive wages from the City.
- We ran a shared folders audit script on the City's domain controller. We analyzed the report, generated by the script, to identify any folders that could potentially have contained files that indicated misuse of City computers. We then determined who had access to those folders and verified the contents of the folders with City officials.
- We reviewed any existing agreements between the City and its IT vendors to determine the scope of services, reporting requirements, performance indicators and security procedures to be provided.
- We asked officials whether the City had a disaster recovery plan.
- We reviewed web filtering settings for City computers to determine whether improper websites were adequately blocked. We also compared website settings to the AUP for compliance to the policy.
- We asked officials whether the City had any written agreements with its banks. We also asked officials whether the City had an online banking policy.

[6] 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 and determined whether there was a proper segregation of duties and whether granted user permissions were necessary for the employees 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 City 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 Council 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 Council to make the CAP available for public review in the City 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