REPORT OF EXAMINATION | 2021M-100

Village of Islandia

Information Technology

NOVEMBER 2021

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

Contents

Report Highlights

Village of Islandia

Audit Objective

Determine whether Village of Islandia (Village) officials ensured information technology (IT) assets were adequately protected from unauthorized access, use and loss.

Key Findings

Village officials did not ensure IT assets were adequately protected from unauthorized access, use and loss. Officials did not:

- Adopt breach notification, password and mobile and removable device IT policies or implement a comprehensive IT contingency plan.
- Monitor and enforce compliance with its acceptable computer use policy (AUP). As a result, we found five of the nine users we audited visited websites for nonbusiness purposes.
- Complete any IT security-related training or provide the opportunity for employees to receive this type of training.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies and a comprehensive IT contingency plan.
- Design and implement procedures to monitor the use of IT resources and provide periodic IT security awareness training to all employees who use IT resources.

Village officials disagreed with certain aspects of our findings and recommendations but indicated they have initiated corrective action. Appendix B includes our comments on issues raised in the Village's response letter.

Background

The Village, located in Suffolk County, is governed by an elected Board of Trustees (Board), which includes the Mayor, the Deputy Mayor and three trustees.

The Board is responsible for oversight and general management and control of finances.

The Village contracts with an IT consultant to perform IT-related services. The IT consultant makes recommendations to the Board regarding hardware and software application acquisitions and/or changes.

During our audit period, the Fire Marshal acted as an IT liaison and, together with the IT consultant, provided general IT support to all departments and employees. The Village has one computer network that contains all user accounts.

Quick Facts	
Employees	45
Network user accounts	37
Servers	1
Computers	16
Computers Reviewed	9
IT Consultant Payments	$55,610

Audit Period

January 1, 2019 – December 31, 2020

Information Technology

The Village relies on its IT assets for Internet access, email, and maintaining financial, personnel, and taxpayer 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 other individuals.

These IT assets must be properly safeguarded to protect PPSI against unauthorized access, misuse and abuse. This is especially important given the increase in attacks including viruses, ransomware and other types of malicious software.

A board should establish security policies for all IT assets and information ... and enforce the policies.

How Should IT Assets Be Safeguarded and Protected?

IT policies, including those related to breach notification, passwords and mobile and removable devices, 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.

Additionally, villages are required 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 PPSI.

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 village data and identifying where it is stored in the computer system and who uses it. Officials should periodically review and update the inventory.

The Board Did Not Adopt IT Security Policies

Village officials did not develop, and the Board did not adopt, breach notification, password and mobile and removable device policies. In addition, officials did not develop a written PPSI policy to define PPSI, explain the reason for collecting PPSI, or procedures for use, access to and storage and disposal of PPSI data. 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 efforts to properly notify affected parties in the event of a

data breach could be hampered. The Mayor said that the Village was unaware of the breach notification policy requirement.

However, without a breach notification policy, the Village may not be able to fulfill its legal obligation to notify affected individuals that they should monitor their credit reports and bank activity because their sensitive and private information was compromised.

Further, 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 procedures for PPSI, there is an increased likelihood that significant errors or fraud could occur and remain undetected.

Why Should the Board Adopt an IT Contingency Plan?

An IT contingency plan is a village's recovery strategy, composed of the procedures and technical measures that enable the recovery of IT operations after an unexpected incident. An unexpected incident could include a power outage, software failure caused by a virus or malicious software, equipment destruction, or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such an event.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the village's computer operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

Because IT often supports key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining a village's critical business processes in the event of a disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Policies and procedures are also critical components and ensure that information is routinely backed up and available in the event of a disruption.

A comprehensive IT contingency plan should focus on strategies for sustaining a village's critical business processes in the event of a disruption.

The IT contingency plan can also include, among other items deemed necessary by the village, the following:

- Roles and responsibilities of key personnel
- Periodic training regarding the key personnel's responsibilities
- Communication protocols with outside parties
- Prioritized mission critical processes
- Technical details concerning how systems and data will be restored
- Resource requirements necessary to implement the plan
- Backup methods and storage policies
- Details concerning how the plan will be periodically tested

The Board Did Not Adopt an IT Contingency Plan

Neither the Board nor the IT consultant developed a comprehensive plan. The Board did not develop a comprehensive IT Contingency Plan (Plan) to describe the measures officials would take to respond to potential disruptions and disasters affecting IT. The Board also did not instruct the IT Director or ask the IT consultant to develop a Plan. As a result, in the event of a disaster, phishing[1] or ransomware attack, staff had no guidance to follow to restore or resume essential operations in a timely manner.

The IT consultant told us that, if a disruption to business continuity or disaster were to occur, he is able and ready to take action to address the situation. However, he has not developed, tested or disseminated a comprehensive contingency plan.

Without a comprehensive plan, there is an increased risk that the Village could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

While the Village's information systems are set to regularly back up the Village's data and store the backups both internally and off-site for up to 60 days, officials did not develop written procedures describing their backup process. Furthermore, although backups are performed, neither the IT consultant nor officials have ever attempted to restore a backup to ensure that the process is functioning as intended and that the data would be available in the event of an emergency.

Without formal written backup procedures, the Village has an increased risk that it could not restore operations quickly and effectively following a service disruption.

Without a comprehensive plan, there is an increased risk that the Village could lose important data and suffer a serious interruption to operations ....

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

Also, without periodic testing of backups, the Board cannot ensure the recovery of necessary data to continue operations if a security breach or system malfunction occurred. Further, without a viable IT contingency plan, the Village is at risk of significant disruptions in business operations after a disastrous event and could suffer unnecessary and preventable losses.

How Should Officials Monitor and Enforce the AUP?

A village 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 IT security policies, AUPs, or standard security practices. Automated mechanisms may be used to perform this process and can help security professionals routinely assess IT security, perform investigations during and after an incident, and even recognize an ongoing attempt of unauthorized access.

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity, or availability. Village 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. 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 village funds.

Officials Did Not Monitor or Enforce the AUP

The Village adopted an AUP in 2011 that defines the procedures for computer and email use. The policy describes what constitutes inappropriate use of IT resources, that there is no expectation of privacy, that all users must responsibly, professionally, ethically and lawfully use the Village's IT resources, and that any violations will be subject to disciplinary action. The AUP requires that each employee sign an acknowledgement form indicating that they have read and understood the policy and agree to be bound by it. Further, the AUP has never been revised, even though the Board re-adopts it every year.

According to the AUP, the Village's IT resources may not be used for the conduct of non-Village business, dissemination or storage of commercial or personal advertisements, private commercial enterprise, solicitations, promotions,

destructive programs…political material, or any other unauthorized use. In addition, IT resources should not be used for, "...material that is fraudulent, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, harassing, discriminatory, offensive, serves no [legitimate] business purpose or is otherwise unlawful or inappropriate…" and that management reserves all rights to determine what constitutes inappropriate or unlawful material.

Figure 1: Examples of Personal Internet Use

Type	Website
Entertainment	healthygeorge.com, pastfactory.com, toocool2betrue.com, youtube.com
News media	investing.com, msn.com, newsday.com
Shopping	amazon.com, bedbathandbeyond.com, cellphonecases.com, chewy.com, kay.com

However, the AUP does not explicitly prohibit incidental and occasional personal use of IT resources.

We reviewed the web browsing history on nine of the Village's 16 computers and found questionable Internet use on eight of the nine computers reviewed.[2] To determine reasonableness of personal use, we reviewed Internet use that exceeded 15 visits to a particular website. We found that on five of the nine computers reviewed, users visited multiple websites more than 15 times each for nonbusiness purposes, including social networking, shopping, entertainment, news, online games and job searches.

Neither Village officials nor the IT consultant implemented any controls to prevent users from accessing nonwork-related websites, such as installing web filtering software, or any other measures to monitor and log network and resource use because officials did not believe that employee Internet use was a significant issue. However, such use can result in unintended consequences and potentially compromise the Village's IT systems. Because officials lack sufficient IT security knowledge, they did not set up the IT system to monitor and log Internet use and were, therefore, unaware of the personal and inappropriate Internet use.

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

2 Refer to Appendix C for information on our sampling methodology.

Why Should Village Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, village officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT resources, 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. In addition, village officials should participate in ongoing IT security training to help ensure they are aware of current trends so they can be sure they have appropriate policies in place and are able to keep them updated as needed.

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 village's IT system and its data. Training programs should be directed at the specific audience (e.g. system users, administrators or officials) and include everything attendees need to perform their jobs.

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

Village officials did not provide users with IT security awareness training ....

Officials Did Not Provide IT Security Awareness Training

Village 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. Furthermore, the Mayor confirmed that officials have not taken training on any IT security-related topics or provided the opportunity for employees to receive this type of training because officials were unaware of the importance of training to help safeguard the Village's IT assets.

Without periodic, formal IT security awareness training Village officials were not aware of the importance of having appropriate IT policies in place and the need to enforce policies. In addition, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, Village data and PPSI could be at greater risk for unauthorized access, misuse, or loss.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT policies to address breach notification, passwords, mobile and removable devices, and communicate the policies to officials, employees and the IT consultant.[3]

2. Review, update and re-adopt its AUP and establish procedures to ensure compliance.

3. Develop a PPSI policy, inventory PPSI and periodically review and update the inventory.

4. Develop a comprehensive IT contingency plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure that it works as intended.

5. Attend IT security awareness training routinely to stay aware of current security risks and how to avoid them.

Village officials should ensure the IT consultant:

6. Designs and implements procedures to monitor the use of IT resources, including personal use, for compliance with the Village's AUP.

Village officials should:

7. Provide periodic IT security awareness training to all personnel who use IT resources.

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

Appendix A: Response From Village Officials[4]

Village of Islandia

1100 Old Nichols Road
Islandia, New York 11749
Tel: 631-348-1133
Fax: 631-348-7650

By email to: Muni-Hauppauge@osc.ny.gov

October 13, 2021

Ira McCracken
Chief Examiner
Office of the New York State Comptroller
New York State Office Building
250 Veterans Memorial Highway
Room 3A10
Hauppauge, New York 11788

Re: Village of Islandia
Response to Draft Audit Report
Information Technology 2021M-100
and Corrective Action Plan

Dear Mr. McCracken:

The Office of the New York State Comptroller issued a draft audit report 2021M-100 (the "Report") resulting from a review of the Village of Islandia Information Technology matters for the period of January 1, 2019 through December 31, 2020 (the "Audit").

The Audit contained three findings and two recommendations which the Village of Islandia (the "Village") will address in this response. The Report otherwise largely consists of statements of policy of the Office of the New York State Comptroller ("Office of the Comptroller") that are relevant to all municipal organizations in New York State but which are not specific to the review of the information and technology matters of the Village that was performed by the Office of the Comptroller.

The Village does have an Equipment and Vehicle Policy and Computer and Telecommunications Use Policy which was previously adopted by the Village under the instruction of the Office of the Comptroller. The existing policy in error is not mentioned in the Report. The representatives of the Office of the Comptroller that performed the Audit advised the Village that the policy must be updated to reflect new positions taken by the Office of the Comptroller. The information on the site of the Office of the Comptroller can only be found after several layers of searches, and the information when found was already nearly four years old and did not match up with the information provided in the Report. There are other factual inconsistencies between the Report and the actual facts of the Village are detailed in this response.

See Note 1 Page 13

Website: newvillageofislandia.com

4 The District's response letter refers to an attachment that supports the response letter. Because the District's response letter provides sufficient detail of its actions, we did not include the attachment in Appendix A.

Key Findings

Finding 1.; Officials did not Adopt breach notification, password and mobile and removable device IT policies or implement a comprehensive IT contingency plan.

Village Response to Finding 1.
This finding is factually incorrect for the reasons stated below.

Breach Notification
The Village by contract developed an agreement with a high level information technology consulting corporation, [redacted], which agreement covers these points and many of the other points that are raised in the Report.

See Note 2 Page 13

There is in fact a breach notification plan in effect whereby the Village is to be notified by [redacted], with specific contacts indicated, if a breach occurs, in order to take appropriate action including but not limited to notification to any affected party or entity. This plan was not stated in the prior Information Technology policy because it was by agreement between the Village of Islanda and its IT consultant vendor, [redacted].

In order to meet the recommendations of the Office of the Comptroller, the breach notification plan is stated in a modified Information Technology Policy that the Village of Islandia will be adopting at this time as part of a corrective action plan ("CAP"). The policy is attached to the Corrective Action Plan ("CAP") which in turn is annexed to this response.

Password and mobile, and removable device IT policies.
This finding is also incorrect. The Village has a password policy which is that each user has an independent confidential password. By policy, the only person that has access to the passwords is the IT Vendor. The representatives of the Office of the Comptroller recommended to the Village [redacted] other measures which the Village is implementing in the CAP, to meet the recommendations of the Office of the Comptroller, however, the Village did have a password policy contained in the current Equipment and Vehicle Policy and Computer and Telecommunications Use Policy. The Village also has a policy regarding mobile and removable devices which is contained in the existing Policy, however the Village will be adopting an updated version of that policy to meet the additional 2018 recommendations of the Office of the Comptroller. The Village is restating these policies in the CAP and the policy to be adopted under the CAP.

See Note 3 Page 13

Implement a comprehensive IT contingency plan.
The Village has an IT contingency plan by agreement with [redacted]. The Village by the CAP will make the plan part of the Village IT Policy.

See Note 4 Page 13

Finding 2. Officials did not monitor and enforce compliance with its acceptable computer use policy (AUP).

Village Response to Finding 2.
The Village of Islandia has the necessary policy prohibiting this use. The Village does not have the sophisticated equipment that is necessary to "monitor and enforce compliance" with the policy, which is a significant expense. The Village has received a quotation from [redacted] for the training and also for software that will monitor this use and that software will be installed and the training provided in conjunction with the CAP. The Village will adopt a policy requiring training and will retrain the full time employee and three part-time employees that work for the Village regarding this point and has addressed this training with [redacted]. [redacted] will be providing the training required and a proposal to technologically restrict this use by adding new software in accordance with a provision of the CAP which will address this point.

See Note 5 Page 13

Finding 3. Officials did not complete IT security related training or provide the opportunity for employees to receive this type of training.

Village Response to Finding 3.
Since there is no assistance with IT security provided by the Office of the Comptroller (there was stated to be a webinar available in the near future however the date and the link were not known to the Office of the Comptroller and there was no announcement to the municipalities that could take advantage of such a training to avoid criticism from the Office of the Comptroller), the Village has received informational training directly from the IT consulting company. Members of the staff have acquired training from sources that have as their goal to provide information and training to villages, such as the New York Conference of Mayors.

See Note 6 Page 13

Due to the limited number of office staff (one full time and three part time) of the Village and the Mayor as the contact, the value of the training program for staff specified by the Office of the Comptroller is not clear. The IT Consultant has been providing training and servicing whenever necessary.

The Village has obtained a proposal from [redacted] which was combined to the CAP, and those actions are in the process of being implemented.

Key Recommendations

Recommendation 1; Adopt comprehensive IT policies and a comprehensive IT contingency plan.

Response to Recommendation 1;
The Village already has an Equipment and Vehicle Policy and Computer and Telecommunications Use that contains many of the points that the Office of the Comptroller recommended however as a CAP the Village has drafted and will be adopting a new Electronic Equipment and Information Technology Policy which will include all of the points recommended in the 2018 information provided by the Office of the Comptroller and the Report as well as the points addressed by [redacted] in a quotation received by the Village.

See Note 1 Page 13

Recommendation 2; Design and implement procedures to monitor the use of IT resources and provide periodic IT security awareness training to all employees who use IT resources.

Response to Recommendation 2;
The Village as provided in the CAP will provide training to employees and officials. The Village has also drafted and will be adopting new procedures and a new Electronic Equipment and Information Technology Policy which will include all of the points recommended in the 2018 information provided by the Office of the Comptroller and the Report with the recommended training to the limited number of employees who use IT resources.

See Note 1 Page 13

Sincerely,

Mayor Allan Dorman
Board of Trustees
Village of Islandia

Appendix B: OSC Comments on the Village's Response

Note 1

Our report refers to the acceptable computer use policy (AUP) the Village adopted in 2011 (refer to page 5 of this report). While the AUP was provided to us during our audit, Village officials did not provide or mention the existence of any other IT use policies. After receiving the Mayor's written audit response, we asked officials to provide the Equipment and Vehicle and Computer and Telecommunications Use policies, but officials did not provide either policy.

All IT guidance provided to the Village and used in our report is from the 2019 documents available at www.osc.state.ny.us/local-government/publications.

Note 2

The Village's agreement with this consulting corporation does not mention breach notification. Any breach notification plan included in this agreement would not constitute a formal written policy duly adopted by the Village Board in accordance with New York State Technology Law, Section 208.

Note 3

Officials stated that additional password and mobile device policies are contained within the Equipment and Vehicle Policy and Computer and Telecommunications Use Policy. However, officials did not provide us with a copy of either of these policies.

Note 4

The agreement provided between the Village and the IT consulting corporation states that the consulting corporation will provide disaster recovery implementation and testing at an additional cost. Officials could not provide an IT contingency plan and the agreement does not state that the consulting firm will develop an IT contingency plan. It also does not specify the additional cost or indicate that the Village exercised this option.

Note 5

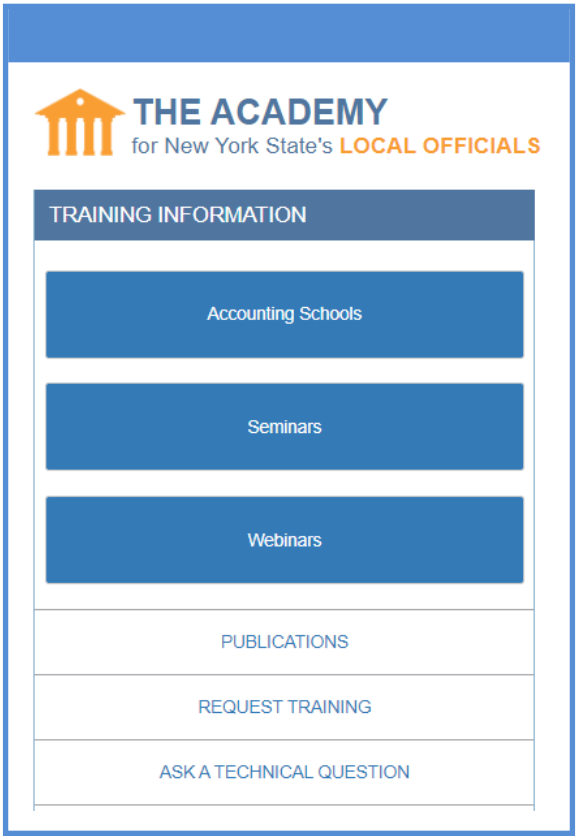
Our audit does not make any recommendations that would require costly sophisticated equipment. The IT consultant agreed the Village can monitor and enforce compliance with its computer use policy by properly configuring its existing firewall.

Note 6

In May 2021, during the audit process, we provided Village officials with our publication *Information Technology Governance* in response to the Mayor's request for IT guidance. Within this publication, audit staff members highlighted a

specific page with a bulleted list of sources of IT security and awareness training, including OSC sources and several external sources.

In addition, OSC released a four-part series of on-demand cybersecurity webinars in October 2020 and another in October 2021. We informed the Mayor and Treasurer about these scheduled webinars on October 6, 13, 20 and 26, 2020 and October 4 and 8, 2021.



Additionally, OSC provides training and assistance on several topics, including cybersecurity, through The Academy for New York State's Local Officials (The Academy). OSC's Local Official Training Unit (LOT) informs both the Mayor and Treasurer of every available webinar ahead of its release by email.

Village officials can access webinars and other training, ask technical questions, and request training on any topic via The Academy website at www.osc.state.ny.us/local-government/academy.

Furthermore, Village officials can always contact the LOT directly by email at localgov@osc.ny.gov or by phone at (866) 321-8503, option 5, with any questions or training requests. Village officials can also contact our Hauppauge Regional Office at any time with any questions that they might have.

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 the Village's employee handbook and IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We reviewed a list provided by the Village that showed the employees who signed acknowledgements stating that they had read the employee handbook and IT Policy. We reviewed all 37 employees during the audit period. We reviewed the acknowledgments for our sample to determine whether 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 Village officials and the Village's IT consultant to gain an understanding of the IT environment and internal controls over IT assets.
- We used our professional judgment to select a sample of nine computers from the Village's 16 computers. We selected computers of users who had access to PPSI and software programs with known vulnerabilities. We reviewed web history reports from these computers to evaluate whether Internet use complied with the AUP.
- We ran a computerized audit script on our sample of nine computers to analyze the Village's network information and determine whether user accounts were necessary. We reviewed user accounts and compared them to a list of current employees to determine whether any network users were no longer employed by the Village. We interviewed Village officials to determine the necessity of any such identified accounts.
- We ran a specialized shared folders audit script on our sample of nine computers to identify any folders that could potentially have contained files that indicated misuse of Village computers. We then determined who had access to those folders and verified the contents of the folders with Village officials.
- We ran a specialized windows audit script on our sample of nine computers to identify unnecessary network and local administrative permissions. We then determined whether these users could make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

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 Village officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Village Board to make the CAP available for public review in the Village Clerk's office.

Appendix D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

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

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

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

Contact

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

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

www.osc.state.ny.us/local-government

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties

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