



# Village of Pelham Information Technology

## Report of Examination

Period Covered:

June 1, 2015 — August 11, 2016

2016M-410



Thomas P. DiNapoli

# Table of Contents

	Page
<b>AUTHORITY LETTER</b>	1
<b>INTRODUCTION</b>	2
Background	2
Objective	2
Scope and Methodology	2
Comments of Village Officials and Corrective Action	3
<b>INFORMATION TECHNOLOGY</b>	4
Monitoring Acceptable Use	4
Breach Notification Policy	5
Disaster Recovery Plan	5
Service Level Contract	6
Recommendations	6
<b>APPENDIX A</b> Response From Village Officials	7
<b>APPENDIX B</b> Audit Methodology and Standards	10
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	11
<b>APPENDIX D</b> Local Regional Office Listing	12

# State of New York Office of the State Comptroller

---

## **Division of Local Government and School Accountability**

April 2017

Dear Village Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and Village Board governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Village of Pelham, entitled Information Technology. This audit was conducted 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.

This audit's results and recommendations are resources for local government officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller  
Division of Local Government  
and School Accountability*

# Introduction

## Background

The Village of Pelham (Village) is located in the Town of Pelham in Westchester County, has an area of 0.8 square miles and a population of about 6,900. The Village provides services for its residents, including police, fire, public works and general government support. Village budgets for the fiscal years ending May 31, 2016 and May 31, 2017 were \$13.7 million and \$13.9 million, respectively.

The Village is governed by an elected Board of Trustees (Board), which is composed of six trustees and a Mayor who serves as chief executive officer. The Board is the legislative body responsible for overseeing Village operations, including establishing internal controls over information technology (IT). The Village is managed by a Village Administrator/Treasurer, who serves as the liaison to the Board and is responsible for the Village's day-to-day operations.

The Village contracts with an IT consultant (service provider) who reviews and updates the Village's computer systems to ensure system and hardware versions are current and performs problem solving on an on-call basis. The Village Administrator/Treasurer serves as the administrator of the Village's financial software.

## Objective

The objective of our audit was to determine whether Village officials adequately safeguarded sensitive data stored on Village computer systems. Our audit addressed the following related question:

- Has the Board implemented effective internal controls over IT to ensure that Village IT assets and computer data are safeguarded?

## Scope and Methodology

We examined the Village's internal controls over IT for the period June 1, 2015 through August 11, 2016. 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 our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report. 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.

**Comments of  
Village Officials and  
Corrective Action**

The results of our audit and recommendations have been discussed with Village officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Village officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

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 forwarded to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Board to make this plan available for public review in the Clerk's office.

## Information Technology

The Village relies on its IT system to perform a variety of tasks, including Internet access, storing data, email communication, recording financial transactions and reporting to State and federal agencies. The Village's IT system and the data it holds are valuable resources that need to be protected from unauthorized, inappropriate and wasteful use. Even small disruptions in IT systems can require extensive time and effort to evaluate and repair. Village officials are responsible for designing and implementing policies and procedures to mitigate these risks. Protecting IT assets is especially important as the number of instances of people with malicious intent trying to harm computer networks or gain unauthorized access to information through viruses, malware and other types of attacks continues to rise.

Village officials have not implemented appropriate policies and procedures for monitoring acceptable use as defined by Village policy, breach notification or disaster recovery, and have not entered into a formal contract with the Village's IT service provider. Consequently, there is an increased risk that productivity could be reduced, IT assets and information could be compromised and affected individuals may not be notified. In addition, the Village could suffer interruption of operations and there could be a lack of individual accountability for various aspects of the IT environment.

### **Monitoring Acceptable Use**

Due to the global nature of the Internet, municipalities find that it is a nearly indispensable resource for conducting business activities. However, even experienced users have been susceptible to significant threats from cybercriminals who exploit the vulnerabilities of systems and software to gain unauthorized access to sensitive data. For example, computers can be infected by malicious software that, unknown to users, installs a keystroke logger that can capture computer user identification and password information. Hackers can later use this information to access networks, databases and even bank accounts, resulting in a high risk of loss. Internet browsing increases the likelihood of exposure to malicious software that may compromise data confidentiality. Village officials should ensure that there is an adequate web filtering process and procedures to limit vulnerabilities through web browsing and ensure the Village's network is only used for job-related purposes.

The Village's acceptable use policy in its Employee Handbook provides guidelines for IT asset use and security and states that the Village's computer systems are Village property and are to be used for job-related purposes. Inappropriate uses explicitly identified

in the policy include, but are not limited to, using the Village's computer, email, wireless network and devices for personal business. However, we examined the web history for five computers and found that employees accessed websites unrelated to Village activities, such as personal business including shopping, travel, sports, social networking and entertainment.

This occurred because the Village has not installed an adequate web filtering process and not adopted procedures to adequately monitor IT usage and enforce compliance with the acceptable use policy. When employees access websites for nonbusiness or inappropriate purposes through the Village's network, productivity is reduced and there is an increased risk that Village assets and users' information could be at risk of compromise through malicious software infections.

### **Breach Notification Policy**

New York State Technology Law requires municipalities and other local agencies to have a breach notification policy or local law. Such policy or local law must require certain individuals be notified when there is a breach of the security of the system as it relates to private information. Private information is defined as information that, if lost, compromised or disclosed, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual. Private information includes social security numbers, bank account numbers, healthcare information, credit and debit card numbers and driver's license information.

The Village Administrator told us that the Village has not adopted a breach notification policy or local law because it was unaware of the legal requirement. As a result, if Village information is compromised, officials and employees may not understand or fulfill their legal obligation to notify affected individuals.

### **Disaster Recovery Plan**

A disaster recovery plan prepares government personnel for the actions they must take if an unexpected event occurs. A disaster recovery plan refers to plans, policies, procedures and technical measures that enable the recovery of IT operations after an event such as a major natural disaster (e.g., a flood), or something smaller, such as human error, hardware failure or malfunctioning software caused by malware or a computer virus. The content, length and resources to prepare a plan will vary depending on the size of the organization's computerized operations. Some best practices include:

- Assembling a team for drafting a disaster recovery plan.
- Identifying and prioritizing critical business processes and services.



- Developing and distributing the plan to responsible parties.
- Training personnel to execute the plan.
- Testing the plan.
- Reviewing and revising the plan to ensure it still meets organizational needs.

The Board has not developed a disaster recovery plan because it has not focused on the disruption of Village business that could occur if the IT systems were rendered inoperative. As a result, the Village could lose important data and suffer a serious interruption in operations.

### **Service Level Contract**

There should be a written contract between the Village and the IT service provider that identifies the Village's needs and expectations and the services to be provided by the independent contractor. The contract should identify the parties to the contract, definitions of terminology, term/duration of contract, scope/subject limitations, service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures, audit procedures, reporting requirements, review/update process, approvals, pricing, billing and terms of payment.

The Board has not negotiated a formal contract with the IT service provider identifying the specific services to be provided or the vendor's responsibilities because it has not considered the benefits of having a contract with the provider. Although Village officials call the vendor when they have questions or issues, the lack of a formal contract could contribute to a lack of protection for the Village and individual accountability for various aspects of the Village's IT environment.

### **Recommendations**

The Board should:

1. Ensure Village officials install an adequate web filtering process and adopt procedures to monitor IT usage and enforce compliance with the Village's acceptable use policy.
2. Adopt a breach notification policy.
3. Develop a comprehensive disaster recovery plan.
4. Develop a formal contract with the Village's IT service provider stating the services to be provided and vendor's responsibilities.

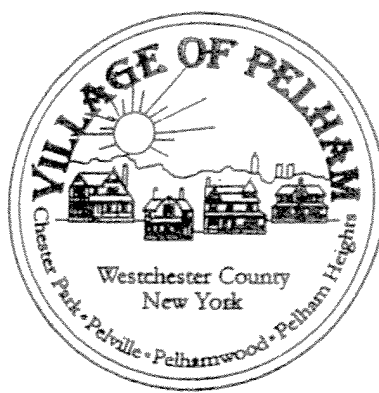


## **APPENDIX A**

### **RESPONSE FROM VILLAGE OFFICIALS**

The Village officials' response to this audit can be found on the following pages.

Michael J. Volpe  
Mayor



Robert A. Yamuder  
Administrator

February 24, 2017

Chief Examiner Tenneh Blamah  
New York State Office of the State Comptroller  
33 Airport Center Drive  
Suite 103  
New Windsor, NY 12553-4725

**Re: Village of Pelham  
Information Technology Security Controls  
Draft Audit Report 2016M-410 for period June 1, 2015 through August 11, 2016**

Dear Chief Examiner Blamah:

On behalf of the Village of Pelham, I am writing to acknowledge receipt of the Office of the State Comptroller's Report of Examination of Information Technology Security Controls of the Village of Pelham for the period from June 1, 2015 through August 11, 2016. The following constitutes the Village's response, including our formal Corrective Action Plan as required. As expressed during the exit conference on February 10, 2017, the Village appreciates the time, effort and guidance of your staff throughout the entire audit process.

## **CORRECTIVE ACTION PLAN**

For each recommendation included in our audit report, the following is our corrective action(s) taken or proposed:

1. Ensure Village officials install adequate web filtering process and adopt procedures to monitor IT usage and enforce compliance with the Village's acceptable use policy.

The Village of Pelham is researching the most effective web filtering software to install on its computer network with input from: 1) Westchester County's Department of Information Technology (DoIT) as they manage the Village's Wide Area Network (WAN) including the firewall protection system; and 2) from the Village's IT consultant Next Step Computers, Inc. The Village is budgeting sufficient funds in the upcoming Fiscal Year 2017/18 budget to purchase appropriate web filtering software in June 2017.

The Village of Pelham is compiling procedures to be formally adopted by a Board of Trustees resolution to monitor employee IT usage and enforce compliance with the Village's IT

use policy which was adopted by the Board of Trustees on June 3, 2014 and appears in the Employee Handbook under “Employee Conduct” section covering: 1) Use of Computer and Electronic Communications Resources; 2) Policy Governing the Use of Social Media; and 3) Conducting Non-Village Business.

2. Adopt a breach notification policy.

On December 6, 2016, the Board of Trustees of the Village of Pelham voted affirmatively to approve by resolution the adoption of “Cyber Incident Response Policy”.

3. Develop a comprehensive disaster recovery plan.

The Village of Pelham is developing a comprehensive disaster recovery plan with input from the Village’s IT consultant Next Step Computers, Inc. The main part of aforementioned recovery plan entails a “Cloud-based” system to remotely back-up the Village’s computer network. The Village is budgeting sufficient funds in the upcoming Fiscal Year 2017/18’s budget to purchase a “Cloud-based” network back-web system in June 2017.

4. Develop a formal contract with the Village’s IT service provider stating the services to be provided and vendor’s responsibilities.

On February 7, 2017, the Board of Trustees of the Village of Pelham voted in favor of adopting a resolution to secure a “Computer Service Agreement” between the computer service provider and the Village of Pelham. A “Computer Service Agreement” was executed accordingly.

Again, the Village of Pelham would like to thank you and your staff for your recommendations and expertise. Our goal in local government is to efficiently manage operations and provide transparency, while ensuring our residents continue to receive excellent service at the lowest possible cost.

Sincerely,

Michael J. Volpe  
Mayor

## **APPENDIX B**

### **AUDIT METHODOLOGY AND STANDARDS**

The objective of our audit was to determine whether the Village adequately safeguarded sensitive data stored on Village computer systems. To accomplish our audit objective and obtain relevant audit evidence, our procedures included the following:

- We examined written Board policies to identify the policies officially adopted for the protection of sensitive data.
- We interviewed Village officials to determine the safeguards in place to protect sensitive data.
- We selected a judgmental sample of five computers based on their access to sensitive information. We searched for website categories that appeared to be personal in nature rather than for Village business to identify questionable Internet use.
- We reviewed the level of services provided by the IT service provider and inquired to determine if there was a formal contract with the provider.

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.

## **APPENDIX C**

### **HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT**

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller  
Public Information Office  
110 State Street, 15th Floor  
Albany, New York 12236  
(518) 474-4015  
<http://www.osc.state.ny.us/localgov/>

**APPENDIX D**  
**OFFICE OF THE STATE COMPTROLLER**  
**DIVISION OF LOCAL GOVERNMENT**  
**AND SCHOOL ACCOUNTABILITY**

Andrew A. SanFilippo, Executive Deputy Comptroller  
Gabriel F. Deyo, Deputy Comptroller  
Tracey Hitchen Boyd, Assistant Comptroller

**LOCAL REGIONAL OFFICE LISTING**

---

**BINGHAMTON REGIONAL OFFICE**

H. Todd Eames, Chief Examiner  
Office of the State Comptroller  
State Office Building, Suite 1702  
44 Hawley Street  
Binghamton, New York 13901-4417  
(607) 721-8306 Fax (607) 721-8313  
Email: [Muni-Binghamton@osc.state.ny.us](mailto:Muni-Binghamton@osc.state.ny.us)

Serving: Broome, Chenango, Cortland, Delaware,  
Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

**BUFFALO REGIONAL OFFICE**

Jeffrey D. Mazula, Chief Examiner  
Office of the State Comptroller  
295 Main Street, Suite 1032  
Buffalo, New York 14203-2510  
(716) 847-3647 Fax (716) 847-3643  
Email: [Muni-Buffalo@osc.state.ny.us](mailto:Muni-Buffalo@osc.state.ny.us)

Serving: Allegany, Cattaraugus, Chautauqua, Erie,  
Genesee, Niagara, Orleans, Wyoming Counties

**GLENS FALLS REGIONAL OFFICE**

Jeffrey P. Leonard, Chief Examiner  
Office of the State Comptroller  
One Broad Street Plaza  
Glens Falls, New York 12801-4396  
(518) 793-0057 Fax (518) 793-5797  
Email: [Muni-GlensFalls@osc.state.ny.us](mailto:Muni-GlensFalls@osc.state.ny.us)

Serving: Albany, Clinton, Essex, Franklin,  
Fulton, Hamilton, Montgomery, Rensselaer,  
Saratoga, Schenectady, Warren, Washington Counties

**HAUPPAUGE REGIONAL OFFICE**

Ira McCracken, Chief Examiner  
Office of the State Comptroller  
NYS Office Building, Room 3A10  
250 Veterans Memorial Highway  
Hauppauge, New York 11788-5533  
(631) 952-6534 Fax (631) 952-6530  
Email: [Muni-Hauppauge@osc.state.ny.us](mailto:Muni-Hauppauge@osc.state.ny.us)

Serving: Nassau and Suffolk Counties

**NEWBURGH REGIONAL OFFICE**

Tenneh Blamah, Chief Examiner  
Office of the State Comptroller  
33 Airport Center Drive, Suite 103  
New Windsor, New York 12553-4725  
(845) 567-0858 Fax (845) 567-0080  
Email: [Muni-Newburgh@osc.state.ny.us](mailto:Muni-Newburgh@osc.state.ny.us)

Serving: Columbia, Dutchess, Greene, Orange,  
Putnam, Rockland, Ulster, Westchester Counties

**ROCHESTER REGIONAL OFFICE**

Edward V. Grant, Jr., Chief Examiner  
Office of the State Comptroller  
The Powers Building  
16 West Main Street, Suite 522  
Rochester, New York 14614-1608  
(585) 454-2460 Fax (585) 454-3545  
Email: [Muni-Rochester@osc.state.ny.us](mailto:Muni-Rochester@osc.state.ny.us)

Serving: Cayuga, Chemung, Livingston, Monroe,  
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

**SYRACUSE REGIONAL OFFICE**

Rebecca Wilcox, Chief Examiner  
Office of the State Comptroller  
State Office Building, Room 409  
333 E. Washington Street  
Syracuse, New York 13202-1428  
(315) 428-4192 Fax (315) 426-2119  
Email: [Muni-Syracuse@osc.state.ny.us](mailto:Muni-Syracuse@osc.state.ny.us)

Serving: Herkimer, Jefferson, Lewis, Madison,  
Oneida, Onondaga, Oswego, St. Lawrence Counties

**STATEWIDE AUDITS**

Ann C. Singer, Chief Examiner  
State Office Building, Suite 1702  
44 Hawley Street  
Binghamton, New York 13901-4417  
(607) 721-8306 Fax (607) 721-8313