New York State Comptroller
THOMAS P. DiNAPOLI

Village of Hudson Falls

Information Technology

2025M-10 | April 2025

Division of Local Government and School Accountability

Contents

Audit Results

Village of Hudson Falls

Audit Objective	Audit Period
Did Village of Hudson Falls (Village) officials adequately secure and protect information technology (IT) systems against unauthorized use, access and loss?	June 1, 2023 – September 30, 2024 We extended our audit period through October 8, 2024 to observe physical security over IT assets at the Village.

Understanding the Program

Village officials and employees use Village-owned IT assets (e.g., computers, laptops and tablets) to perform day-to-day operations and access and store information collected by the Village. The Village relies on its IT systems (including its IT assets and network) for Internet access and email, and to maintain various records, such as financial and personnel records and evidence files for the police department, that may contain personal, private or sensitive information (PPSI).[1] If an IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and rebuild.

The Village pays two outside IT vendors to provide IT services for the Village, including managing IT support, monitoring virus protection, network management and other IT-related services.

Audit Summary

The Village Board (Board) and officials did not establish adequate controls to safeguard IT systems or develop adequate IT policies or procedures. In addition, the Board did not develop and adopt an IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of services, periodically test backups or provide IT security awareness training. As a result, Village officials cannot be assured that Village IT systems are secured and protected against unauthorized use, access and loss, and there is an increased risk that officials could lose important data and suffer a serious interruption in operations.

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third-parties or other individuals or entities.

For example, officials did not monitor employee Internet use. Although a June 2001 memo prohibited employees from using Village-owned computers for personal use, officials and employees were not aware of this memo. As a result, the seven employees' Internet histories we reviewed identified that all seven employees used Village computers to access websites for personal use, such as shopping, social media, streaming platforms, entertainment, personal email and finances, food, and personal health and fitness.

In addition, the Board paid two IT vendors for IT services totaling $31,333 during our audit period but did not enter into a written contract or service level agreement (SLA) with the IT vendors that described specific IT services to be provided. Officials did not monitor the services provided by one IT vendor to ensure all the services outlined in the annual invoice were provided.

While the Village's IT assets we examined were physically secured, the server and physical backups were not properly protected from water damage that occurred due to roof construction at the Village Hall. Weaknesses in policies, oversight and other internal controls increase the risk that hardware or software systems may be lost, damaged or compromised by unauthorized or inappropriate access and use.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes nine recommendations that, if implemented, will improve the Village's IT practices to protect against unauthorized use, access and loss. Village officials generally agreed with our findings and indicated they plan to initiate corrective action.

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. Our methodology and standards are included in Appendix C.

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 the New York State 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 the CAP available for public review in the Clerk's office.

Information Technology Findings and Recommendations

A village's IT systems and the data they hold are valuable and need to be protected from unauthorized access, inappropriate and wasteful use or loss. A village board (board) should establish IT policies that take into account people, processes and technology. Specifically, the board should adopt an acceptable use policy that describes appropriate and inappropriate use of IT systems and consequences of violating the policy. The board should communicate these policies to all computer users, ensure officials develop procedures to monitor compliance with the policies and develop and deliver IT security awareness training. More details on the criteria used in this report are included in Appendix A.

Finding 1 – Officials did not monitor employee Internet use.

Although officials set up web filtering software to prevent access to certain websites, including obscene material and unlawful activity, they did not monitor employee Internet use. We reviewed Internet history on seven Village computers assigned to seven employees, and determined that all seven computers were used to access websites for personal use, such as shopping, social media, streaming platforms, entertainment, personal email and finances, food and personal health and fitness (Figure 1).

Figure 1: Examples of Personal Internet Use

Type	Website
Entertainment	sixflags.com, youtube.com, expedia.com, accuradio.com
Food	subway.com, hannaford.com, chipotle.com, pricechopper.com
Health and Fitness	medentmobile.com, glensfallsymca.org, planetfitness.com, tops.org
Personal Email	mail.google.com, yahoo.com
Personal Finances	tdbank.com, paypal.com, e-zpass.com
Shopping	amazon.com, otterbox.com, staples.com, canva.com
Social Media	facebook.com
Streaming Platforms	netflix.com, spotify.com

Officials initially told us that the Village did not have IT policies. However, they later provided a June 2001 memo addressed to all Village employees with language about acceptable computer use prohibiting employees from using Village-owned computers for personal use. Because the Board and officials were not aware of this memo, it had not been communicated with current Village employees. In addition, because officials did not monitor employee Internet use, they could not determine whether employees were complying with the Village's policy or using the Village's Internet services for personal use.

While web filtering software can help mitigate instances of inappropriate and/or personal Internet browsing, periodic reviews of Internet history would provide a more definitive review of activity to identify inappropriate and/or personal Internet browsing. Further, when formal IT policies are not developed and employees are unaware of the Village's acceptable computer use expectations, there is an increased risk that Village computers could be exposed to malicious content on visited Internet websites that could compromise PPSI or IT systems.

Recommendations

1. The Board should develop and communicate IT policies, including acceptable computer use expectations, to Village employees.
2. Officials should implement procedures to monitor employee Internet use.

Finding 2 – The Board did not enter into a written contract or service level agreement with IT vendors.

The Village paid two IT vendors for IT services totaling $31,333 during our audit period based on invoices with a description of the services provided. For example, one IT vendor sent an annual invoice describing the IT services to be provided for the upcoming fiscal year. The IT vendor was paid for providing assistance with software and hardware setup and maintenance, backup support, monitoring the Village's antivirus software, monthly review of backup and restore functions, management of the Village's identity and access management system, and firmware upgrades to systems, routers and switches. However, officials did not monitor the services provided by the IT vendor to ensure all the services outlined in the annual invoice were provided.

Without a comprehensive written contract and SLA, officials were unaware of the extent of services being provided and could not ensure the Village was receiving the services which it paid for and should have received. Insufficient, nonexistent or vague agreements can contribute to confusion regarding who is responsible for various aspects of the IT environment, which puts data and IT systems at greater risk for unauthorized access, misuse or loss.

Recommendations

The Board should:

3. Enter into a comprehensive written contract with each IT vendor that sufficiently defines the contractual relationship and responsibilities between the IT vendors and the Village.
4. Develop an SLA with each IT vendor that addresses the Village's specific IT service needs and expectations.

Officials should:

5. Monitor services provided by the IT vendor to ensure all services outlined in the annual invoice are provided.

Finding 3 – The Board did not develop an IT contingency plan, periodically test backups or provide IT security awareness training.

Although the Village had an emergency preparedness plan, it did not cover specific procedures to recover from an unexpected IT disruption. In addition, the plan was outdated and not regularly reviewed to ensure pertinent information was updated. The plan was created in December 1993 and included key contacts that were no longer Village employees. Officials told us that the Board does not periodically review the emergency preparedness plan. However, Village police department officials review the plan annually as part of the department's accreditation process. The plan has not been updated since its creation.

On a daily basis, computers connected to the network are backed up, and the backups are stored both onsite and offsite. However, these backups were not periodically tested to ensure that they will function as expected. In addition, officials did not provide IT security awareness training to ensure employees understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the Village's IT systems.

The Village's IT vendor stated that backups are generally restored only when data has been lost or damaged due to a power outage. In addition, officials told us that the Village's computing environment is not often discussed amongst the Mayor and Board Trustees, and officials rely on the IT vendors to perform IT functions.

Without an IT contingency plan, responsible parties may not be aware of the steps they should take or how to continue doing their jobs to resume business in the event of a disaster or other unexpected IT disruption. Also, by not testing backups, Village officials have no assurance that important data will be available in the event of a loss. Further, the failure to provide IT security training and raise awareness increases the risk that users will not understand their responsibilities, putting the data and IT systems at greater risk for unauthorized access, misuse or abuse. As a result, the Village has an increased risk that it could lose important data and suffer a serious interruption in operations.

Recommendations

The Board should:

6. Develop and adopt an IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

7. Ensure IT security awareness training is periodically provided to all individuals who use Village IT resources.

Officials should:

8. Establish procedures to ensure backups are routinely tested.

Finding 4 – Officials did not protect IT assets from water damage.

The Village's IT assets were physically protected from unauthorized access. However, we observed water leakage from the ceiling above the IT assets, including the server and physical backups (Figure 2). Officials stated that the leak occurred overnight due to roof construction being performed at the Village Hall. Officials tarped the IT assets and picked the server up from the damp floor once they were made aware of the water damage (Figure 3).

FIGURE 2: Water Leakage Above IT Assets

Photo taken on October 8, 2024 by OSC auditors with permission from Village officials.

FIGURE 3: Tarped IT Assets to Protect From Water Damage

Photo taken on October 8, 2024 by OSC auditors with permission from Village officials.

The failure to properly safeguard IT assets from environmental hazards such as water damage can result in significant data loss, operational disruption and costly repairs or replacements.

Recommendation

9. Officials should ensure that IT assets are safe from environmental damage, such as water damage.

Multiple security weakness, including relying on IT vendors to perform IT functions without direct communication and a comprehensive written contract or SLA and not establishing other adequate controls to safeguard IT systems, compound the risk of unauthorized access, misuse or loss of information maintained within the Village's IT system.

Appendix A: Profile, Criteria and Resources

Profile

The Village is located in the Town of Kingsbury in Washington County and is governed by an elected Board composed of a Mayor and four Trustees.

The Board is responsible for the general oversight of the Village's operations and finances, which includes maintaining security over the Village's IT system. The Village has approximately 42 employees, 36 enabled network user accounts and 24 network computer accounts (servers, desktops and laptops).

Criteria – Information Technology

Although no single practice or policy on its own can adequately safeguard IT systems from cybersecurity risks, there are several IT governance efforts that, if properly enacted and monitored, collectively increase the odds IT systems will remain safe.

A board should have a comprehensive written contract with its IT vendors that indicates the contract period, services to be provided and basis of compensation for those services. In addition, officials should have a separate written SLA between the village and its IT vendors that identifies the village's needs and expectations and specifies the level of services to be provided. An SLA is different from a traditional written contract in that it establishes comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. Having a written contract and SLA with the IT vendors will allow officials to monitor the IT vendor's work to ensure that the village is receiving all contracted services.

In addition, the board should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. A disruptive event could include a power outage, software failure caused by a virus or malicious software, equipment destruction, inadvertent employee action or a natural disaster, such as a flood or fire, that compromises the availability or integrity of village services, including the IT system and data.

Typically, IT contingency planning involves analyzing business processes and continuity needs, focusing on sustaining critical functions and identifying roles of key individuals and necessary precautions needed to maintain or quickly resume operations. The plan should be periodically tested and updated to ensure officials understand their roles and responsibilities in a disaster situation or other unexpected IT disruption and to address changes in security requirements. In addition, a plan should include data backup procedures and periodic backup testing to help ensure backups will function as intended. To help minimize the risk of a disruption, officials should have periodic IT security awareness training that explains common security threats and the proper rules of behavior for using the Internet and IT resources, systems and data. The training should communicate policies and procedures to all

IT system users so they understand IT security measures and their roles in safeguarding data and IT assets.

To safeguard IT assets from unintentional harm, loss or impairment, IT assets should be in a locked and secured area with environmental controls, such as smoke detectors, fire alarms and extinguishers, and protection from water damage.

Additional IT Resources

FIGURE 4: OSC Publications

OSC Local Government Management Guides available on our website to help officials understand and perform their responsibilities.

Information Technology Governance

https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf

Information Technology Contingency Planning

https://www.osc.ny.gov/files/local-government/publications/pdf/itcontingencyplanning.pdf

The Practice of Internal Controls

https://www.osc.ny.gov/files/local-government/publications/pdf/the-practice-of-internal-controls.pdf

In addition, our website can be used to search for audits, resources, publications and training for officials: https://www.osc.ny.gov/local-government.

Appendix B: Response From Village Officials

JOHN E. BARTON
MAYOR

CASSANDRA A. ALLEN
VILLAGE CLERK-TREASURER

VILLAGE OF HUDSON FALLS
220 Main Street
Hudson Falls, NY 12839
Phone (518)747-5426

TRUSTEES:
JAMES J. GALLAGHER, JR.
MICHAEL L. HORRIGAN
DANIEL F. HOGAN
JEFFREY G GAULIN

MICHAEL J. FIORILLO
SUPERINTENDENT OF PUBLIC WORK
WILLIAM L. NIKAS
VILLAGE ATTORNEY

April 15, 2025

Gary G. Gifford, Chief of Municipal Audits
New York State Comptroller
Glens Falls Regional Office
One Broad Street Plaza
Glens Falls, NY 12801-4396

RE: 2024 Audit, Information Technology
Village of Hudson Falls

Dear Mr. Gifford

On April 1st, 2025, the Village of Hudson Falls received the results of the recent audit performed by the New York State Comptroller's Office. The objective of the audit was Information Technology Systems. The Board collectively accepts the findings of the report and will begin working diligently in correcting the mandatory areas of concern.

Sincerely,

Mayor Barton
Village Mayor

Appendix C: Audit Methodology and Standards

We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed Village officials, employees and IT vendors to obtain an understanding of the Village's IT operations and related policies and procedures and to determine whether the policies and procedures were adequate, an IT contingency plan existed and Village employees received IT security awareness training.
- We physically observed the Village's antivirus software to determine whether the Village's web filter was active and the websites blocked by the web filter.
- We used our professional judgement to select seven employees based on their job titles and duties, which included accessing the Village's accounting system, police evidence and/or building permits and inspections. We ran a computerized audit script on the seven employees' computers on September 30, 2024 and reviewed these employees' Internet history to determine whether employees accessed secured and appropriate websites.
- We reviewed all invoices paid to the IT vendors during our audit period to identify the services provided.
- We physically observed the Village's IT assets to determine whether the Village implemented appropriate physical security controls.
- We analyzed and assessed all 36 enabled network user accounts using a computerized audit script we ran on September 21, 2024 and compared the network user accounts to the Village's organizational chart to determine whether there were any enabled network user accounts assigned to former Village employees.

Our audit also examined the adequacy of certain IT 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 relevant population size and the sample selected for examination.

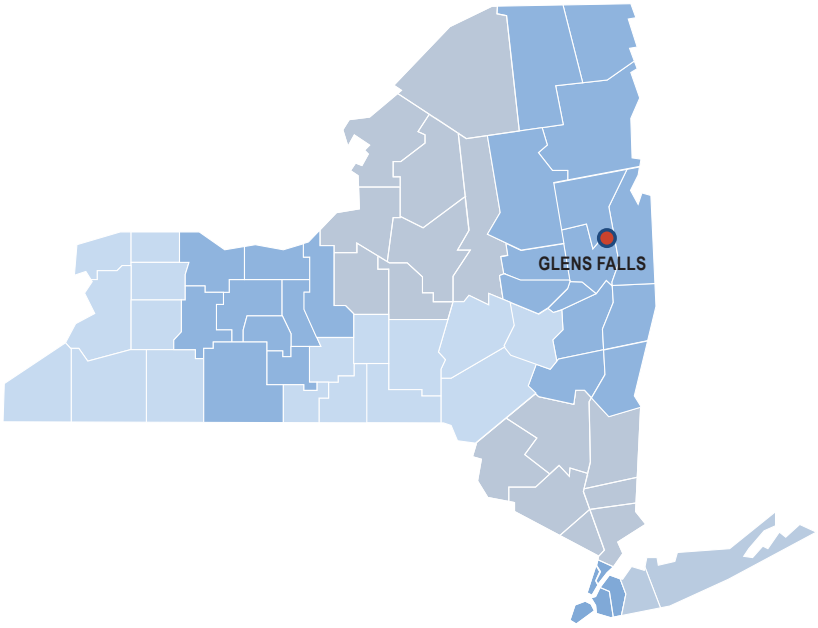
Contact

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford Chief of Municipal Audits

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties



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

https://www.osc.ny.gov/local-government

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