REPORT OF EXAMINATION | 2019M-36

Town of Lloyd

Information Technology

JUNE 2019

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

Contents

Report Highlights

Town of Lloyd

Audit Objective

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

Key Findings

- Employees accessed nonbusiness websites for personal use.
- The Board did not provide IT security awareness training for employees who used Town IT assets.
- Town officials (Officials) did not adopt a disaster recovery plan or develop written data backup procedures.

In addition, sensitive IT control weaknesses were communicated confidentially to Officials.

Key Recommendations

- Monitor compliance with the acceptable use policy.
- Provide IT security awareness training to personnel who use IT resources.
- Adopt written IT policies and procedures to address disaster recovery and data backup.

Officials indicated that they have initiated corrective action.

Background

The Town of Lloyd (Town) is located in Ulster County and serves approximately 11,000 residents.

The Town is governed by an elected five-member Town Board (Board), composed of the Town Supervisor (Supervisor) and four Board members. The Board is responsible for the general oversight of the Town's operations and finances. The Supervisor, as chief fiscal officer, is responsible for the day-to-day management of the Town.

The Town contracted with a third-party consultant to operate and maintain the Town's IT system. The Supervisor is responsible for overseeing the IT consultant.

Quick Facts	
Servers	5
Computers	44
Employees	88
2019 General Fund Appropriations	$5 million

Audit Period

January 1, 2017 – September 14, 2018. We extended our scope period to January 15, 2019 for IT information.

How Does an Acceptable Use Policy Protect IT Assets?

Acceptable use policies describe what constitutes appropriate and inappropriate use of IT resources, along with the Board's expectations concerning personal use of IT equipment and user privacy.[1] Monitoring compliance with the acceptable use policy involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should require employees to sign the policy explaining the information is not private and should not be used for personal purposes.

Officials should monitor and analyze activities for signs of possible violations 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 and can help security professionals routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access.

Officials Did Not Monitor Computer Use

The Board adopted an acceptable use policy that states that computers are to be used for business purposes only. However, Officials did not require users to sign the policy, enforce the policy or design and implement procedures to monitor compliance with the policy to determine the amount of employees' personal use.

We examined ten[2] computers to determine whether they were used for nonbusiness purposes and found evidence of personal use on every computer. Such use included the following:

Figure 1: Examples of Personal Internet Use

Type	Site
Personal Email	Aol.com
Social Networking	Snapchat.com
Gaming	Wineverygame.com
Shopping	Oldnavy.gap.com
Travel	Jetblue.com
News/Entertainment	Dreamindemon.com
Couponing	Groupon.com
Gambling	Officefootballpool.com
Personal Online Banking	Hvfcu.org

1 For example, management may reserve the right to examine email, personal file directories, web access and other information stored on computers, at any time and without notice.

2 Refer to Appendix B for further information on our sample selection.

According to Officials, inappropriate usage was due to having no web filters, and a past practice that allowed unrestricted access to the Internet.

When employees access websites for nonbusiness or inappropriate purposes through the network, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections (malware).

Why Should the Town Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and personal, private and sensitive information (PPSI), Officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet, IT systems and data, and communicates related policies and procedures to all employees. The training should center on emerging trends such as information theft, social engineering attacks[3] and computer viruses and other types of malicious software, all of which may result in PPSI compromise. 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 downloading files and programs from the Internet or portable devices such as thumb drives; the importance of selecting strong passwords; any requirements related to protecting PPSI; the risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

Town Employees Were Not Provided With IT Security Awareness Training

Although the Board has adopted an acceptable use policy, it did not provide users with IT security awareness training to help ensure they understand security measures to protect the network. Officials did not implement training due to limited time and staff.

The failure to provide IT security training increases the risk that users will not understand their responsibilities, putting the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse. Additionally, user's actions can cause significant harm to computer systems or financial losses.

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

Why Should the Town Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, the Board should adopt a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and any PPSI contained therein. Typically, a plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations.

Additionally, Officials should establish data backup procedures that include:

- The frequency and scope of backups,
- The location of stored backup data,
- The specific method for backing up and any other important details relating to the process,
- How the town will periodically verify that the data has been backed up, and
- How it will test its ability to restore backup data.

The Board Did Not Adopt a Disaster Recovery Plan

The Board has not adopted and implemented a written disaster recovery plan. Also, although the Town performs data backups daily, the Board has not established written procedures for how systems are to be backed-up, nor have Officials verified the data and tested the ability to restore the backups.

In the event of a disaster, Town personnel have no guidelines or plan to follow to prevent the loss of equipment and data or appropriately recover data. The lack of a disaster recovery plan could lead to the loss of important data and a serious interruption to Town operations, such as not being able to process payroll or vendor claims.

How Should Officials Maintain Computer Inventory?

Officials should maintain detailed, up-to-date inventory records for all computer hardware. The information maintained for each piece of computer equipment should include a description of the item (make, model and serial number), the name of the employee to whom the equipment is assigned, if applicable, the physical location of the asset and relevant purchase or lease information including the acquisition date.

Officials Did Not Maintain an Adequate Inventory

We reviewed the computer and server inventory lists maintained by the Town and determined there were a total of 41 computers and servers listed. However, we found that there are 44 computers and five servers owned by the Town. We also found that there were incomplete descriptions on the inventory lists.

Figure 2: Inadequate Inventory

Issue:	# of Computers/ Servers	Percentage
Not Listed on Inventory	8	16%
No Make/Model Number	22	54%
No Acquisition Date	24	59%
No Serial Number	15	37%
Inaccurate Serial Number	2	8%

According to the Supervisor, he was unaware the computer equipment inventory was not sufficient and was not accurate as the list is provided by the IT consultant. Without detailed equipment records, it is difficult to verify the existence of the equipment and deter theft and misuse.

What Do We Recommend?

The Board should:

1. Ensure that Officials monitor compliance with the acceptable use policy.
2. Provide IT security awareness training to personnel who use IT resources.
3. Adopt a disaster recovery plan.

The Supervisor should:

4. Require all users to sign the acceptable use policy that explains the information stored is not private and computers should not be used for personal purposes and outline penalties for misuse of equipment.
5. Monitor computer Internet use to ensure employees comply with the acceptable use policy.
6. Establish written data back-up procedures, and periodically test the procedures to ensure that the data is backed up and can be restored.
7. Review and update all equipment inventory records to ensure they are complete and contain accurate and current information.

Appendix A: Response From Town Officials

Town of Lloyd, 12 Church Street, Highland, New York 12528
845-691-2144 Town Clerk, Supervisor, Assessor, Building/Planning/Zoning
Court 845-691-7544 Highway 845-691-7631 Police 845-691-6102 Water/Sewer 845-691-2400

4, June 2019

Office of the State Comptroller
Division of Local Government & School Accountability
Newburgh Regional Office
Attn: James Obeng, Principal Examiner
33 Airport Center Drive
Suite 103
New Windsor, New York 12553-4725

RE: Town of Lloyd – Information Technology
Report of Examination
2019M-36

Dear Mr. Obeng,

This letter shall serve as receipt of the draft report of examination of the aforementioned. In the Key Findings section of the report highlights, the Town of Lloyd has installed and enabled web filtering; trained department heads with regard to IT security awareness and will be adopting and implementing IT policies and procedures to address internet usage, email usage and disaster recovery and backup. Since this review, we had made numerous changes as suggested and will continue to regulate and monitor IT security.

Sincerely for the Town of Lloyd Town Board,

Paul J. Hansut

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the Town's policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed Town officials to gain an understanding of the processes and procedures over the IT system and applications.
- We selected to analyze 10 of the 29 computers from the Town Hall's network.[4] We tested five computers based on users with access to PPSI within the Finance Department and Clerk's Office and then judgmentally selected one computer from each department. We excluded the Police Department based on their need to investigate various topics for cases. We ran a Web History script on our sample of 10 computers (34 percent) to identify any inappropriate use.
- We performed a walk-through to verify the IT asset inventory list.

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 Town 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.

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 Board to make the CAP available for public review in the Town Clerk's office.

4 There are 49 computers owned by the Town and Police Department, 29 on the Town Hall's network and 20 on the police network.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/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/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

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

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/localgov/index.htm

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

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, 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.gov.ny

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

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