REPORT OF EXAMINATION | 2019M-34

Town of Grand Island

Information Technology

AUGUST 2019

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

Contents

Report Highlights

Town of Grand Island

Audit Objective

Determine whether the Board ensured information technology (IT) assets were properly safeguarded.

Key Findings

- Town officials did not monitor Internet usage for computer use policy (CUP) compliance.
- Town officials did not review the inventory of IT hardware and do not maintain an inventory of software or data.
- Town employees were not provided with IT security awareness training.

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

Key Recommendations

- Design and implement procedures to monitor Internet usage for CUP compliance.
- Periodically review the inventory of IT assets and expand it to include software and data.
- Ensure that all necessary Town personnel receive IT security awareness training and that training is provided whenever the IT policies are updated.

Town officials did not agree with certain aspects of our findings and recommendations but indicated that they plan to initiate corrective action. Appendix B includes our comments on the issues raised in the Town's response.

Background

The Town of Grand Island (Town) is located on a 28.5 square mile island in Erie County.

The Town is governed by an elected Board (Board), which is composed of a Supervisor and four Council members. The Board is responsible for the general oversight of operations and finances including establishing policies and procedures to safeguard IT assets and provide a secure IT environment. The Supervisor is responsible, along with other Town officials, for the day-to-day management of the Town.

The Town contracts with an IT Consultant to oversee the Town's IT environment. The IT Consultant reports to the Town Accountant.

Quick Facts	
2019 General Fund Appropriations	$8.4 million
Employees	140
Computers	81
Servers	3 physical 19 virtual

Audit Period

January 1, 2017 – December 12, 2018

Information Technology

The Town relies on its IT systems for Internet access, email, and maintaining and accessing personal, private or sensitive information (PPSI)[1] including financial and personnel records. Therefore, the IT systems and data are valuable Town resources. If IT systems are compromised, the results could range from inconvenient to severe and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of an IT system, a lack of effective controls significantly increases the risk that data, hardware and software may be lost or damaged.

How Should IT Assets Be Safeguarded?

It is essential that a board establish policies for online banking and remote access. An online banking policy should include the online banking activities the town will engage in, the employees with authority to process transactions and an approval process.[2] A remote access policy should include which employees are authorized to have remote access, information on the necessity for their job duties and an approval process. In addition, New York State Technology Law[3] requires a town to have a breach notification policy or local law that requires certain individuals to be notified when there is a system security breach involving private information.

Town officials should disable or remove the accounts of those who have left town employment or transferred to another area. In addition, they should determine whether accounts that are not used frequently[4] are necessary or should be disabled or removed. Some generic accounts[5] may be unnecessary and can inadvertently grant users more access than needed. In addition, the Board adopted a CUP that states user accounts are for Town related purposes and that users shall not use the Town-owned computers for non-Town activities.[6] Town officials should monitor for CUP compliance and maintain detailed, up-

1 PPSI is any information that – if subjected to unauthorized access, disclosure, modification, destruction or disruption of access or use – could severely affect critical functions, employees, customers, third parties or residents of New York State in general.

2 See our publication, *Cash Management Technology*, for additional guidance: https://www.osc.state.ny.us/localgov/pubs/lgmg/cashtechnology.pdf

3 New York State Technology Law Section 208

4 Accounts that have not been accessed for six months or more

5 Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled or removed, if necessary.

6 The CUP established that authorized representatives of the Town may intercept, monitor the use of such equipment including Internet files and that employees should expect no privacy when using the computer system.

to-date inventory records[7] for all computer hardware, software and data and provide periodic IT security awareness training.[8] Security awareness training communicates expectations to employees, helps them recognize security concerns and react appropriately, and helps them understand their individual responsibilities.

Finally, officials should establish a written disaster recovery 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 financial system and any PPSI contained therein. Typically, a disaster recovery plan involves the analysis of business processes and continuity needs, the roles of key individuals and the precautions to maintain or quickly resume operations.

Officials Have Not Developed Adequate IT Policies

Online Banking – The Board has not adopted a written online banking policy. Although Town officials have unwritten electronic banking procedures, partly put in place by the Town's bank, a written policy assigning personnel to authorize and approve transactions, transmit, record and review electronic banking transactions would provide assurance that proper procedures continue in the event of personnel changes.

Remote Access – The Board did not adopt a written remote access policy. Employees are granted remote access on a case-by-case basis, but there is no documentation to identify who has remote access, why it is necessary for their job duties and who approved it. A review of service call tickets from January 1, 2017 through September 2018 identified eight service requests for installation of remote access to the Town's network. The Town Accountant told us that the IT Consultant will not set up remote access without her approval; however, there was no documentation of this approval.

Breach Notification – The Board and Town officials have not developed and adopted a written breach notification policy or local law because they were unaware of this requirement. As a result, if PPSI is compromised, officials may not fulfill the Town's legal obligation to notify affected individuals.

7 This information should include a description of the item including the make, model and serial number; the name of the employee to whom the equipment is assigned; the physical location of the asset; and purchase or lease information including the acquisition date. Software inventory records should include a description of the item including the version and serial number, a description of the computers on which the software is installed and licensing information.

8 Training should also be provided whenever the IT policies are updated.

Officials Have Not Monitored User Accounts

We reviewed all 219 enabled accounts on the Town's network and found that 109 (50 percent) had not been used in more than six months. These user accounts consisted of 43 generic accounts set up for use by Town departments, vendors and the general public, 61 employee and five vendor accounts. Of the 61 employee accounts, 33 (54 percent) have never been used and of the 48 generic/vendor accounts, 29 (60 percent) have never been used. While some accounts may be needed for current employees or operations, others may be unnecessary and should be disabled.

Officials told us they used service tickets to notify their IT Consultant when employees left Town employment but were unaware that these accounts were not disabled or removed. For eight of the recent employee separations,[9] we identified five service tickets requesting restricted user access and removal of credentials. Despite being active, those employees could no longer access the network using these accounts. However, no service tickets were identified for the remaining three employee separations and there is a risk those former employees could still access the network using these three accounts. User accounts of former employees that have not been disabled or removed could be used by those individuals or others for malicious purposes. Further, unnecessary accounts create additional work to manage network access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

Town Computers Were Used for Personal Activities

Although the CUP is in the Town's employee manual and is annually reaffirmed and generally signed[10] by each employee, we identified personal Internet use on all seven computers[11] we examined. Such use included online shopping, personal email, social networking, web browsing for job searches, travel and real estate and nonbusiness related document file downloads and video streaming.

Town officials were unaware of the personal computer use because they do not routinely monitor employee Internet usage for CUP compliance. When employees access websites for nonbusiness or inappropriate purposes, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections.

9 Employees who left service between October 2017 and May 2018, including six employees and two Board members with expired terms

10 Signature indicates that employee has received and read the CUP and that it is the employee's responsibility to follow the policy.

11 See Appendix C, Methodology and Standards, for information about the sample

Officials Did Not Maintain an Accurate Inventory of IT Assets

The IT Consultant maintains an inventory of IT hardware for the Town and periodically sends officials a copy for their review. However, Town officials did not periodically review the inventory. In addition, they also do not maintain a software and data inventory. There were 75 computers on the IT Consultant's inventory that were listed as active. We examined Town assets and identified six active computers which were not on the inventory list. In addition, 10 computers were assigned to different users than listed on the inventory.

Without accurate hardware, software and data inventory records, unauthorized devices and software can be easily introduced. As a result, there is an increased risk of loss, theft or misuse of IT assets.

Employees Were Not Provided With IT Security Awareness Training

Town employees were not provided with IT security awareness training. By not providing IT security training, there is an increased risk that users will not understand their responsibilities, putting data and computer resources at greater risk for unauthorized access, misuse or abuse.

The Board Has Not Adopted a Written Disaster Recovery Plan

While Town officials have worked with the IT Consultant to implement certain components of a disaster recovery plan, they have not developed a written plan to present to the Board. Without a formal written plan, responsible parties may not be aware of steps they should take, or how to continue doing their jobs, to resume business after a disruptive event.

What Do We Recommend?

The Board and Town officials should:

1. Develop and adopt written online banking, remote access and breach notification policies and related procedures.
2. Disable or remove unnecessary network user accounts and conduct periodic reviews for any unnecessary accounts.
3. Monitor Internet usage for CUP compliance.
4. Periodically review and update the inventory of IT assets and expand it to include software and data.
5. Ensure employees are provided with IT security awareness training and that additional training is provided whenever the IT policies are updated.

The Board should:

6. Adopt a written disaster recovery plan.

Appendix A: Response From Town Officials

THE TOWN OF _____ GRAND ISLAND

NATHAN McMURRAY *Supervisor*
PATRICIA A. FRENTZEL *Town Clerk*

BEVERLY KINNEY
MIKE MADIGAN
JENNIFER L. BANEY
PETER MARSTON JR.
Councilmembers

2255 BASELINE ROAD
GRAND ISLAND
NEW YORK
14072-1710
OFFICE (716) 773-9600
FAX (716) 773-9618

August 16, 2019

Office of the State Comptroller
Division of Local Government & School Accountability
PSU-CAP Submission
110 State Street, 12th Floor
Albany, NY 12236

RE: Town of Grand Island – Report #2019M-34 – Response

Dear Sir or Madam:

On behalf of the Town Board and other officials of the Town of Grand Island, I would like to thank your office, and particularly your examiner, [redacted] for her courtesy and professionalism in conducting a review of our Town's Information Technology.

Your report noted three key findings:

1. ***Town officials did not monitor internet usage for Computer Use Policy (CAP) compliance.***

While the Town does not monitor employee's internet usage routinely, we have Content Filtering in place to restrict certain sites and provide a source to investigate abuse on a case by case basis. Town officials will review our CAP and Monitoring procedures, and make changes as appropriate.

2. ***Town officials did not review the inventory of IT hardware and do not maintain an inventory of software or data.***

See Note 1 Page 9

We disagree with the characterization. The Town DOES review the inventory of IT hardware. Of the six (6) computers identified, the majority were either not in use, or property of/or provided by/ another entity (such as NYS Court Admin). None of the exceptions noted were of IT Equipment that was "lost" in any way (i.e. on the list but not able to be located). Town Officials will address corrections, and inventory of software and data. 2018 was unique, in that the inventory list had not been scrutinized and updated on its normal annual review schedule.

3. ***Town employees were not provided with IT security awareness training.***

Town officials began discussing IT Security Awareness Training with our Vendor in mid-2018. However due to other priorities, and this OSC Audit being conducted where other recommendations may well have impacted training choices, we decided to postpone a decision on implementation until 2019. The Town agrees with the findings, and will develop a plan to put such training(s) in place.

With regard to the comment about user accounts/monitoring, we absolutely agree that user accounts should be deactivated or otherwise protected when no longer needed. However, implying that accounts not logged into for over six (6) months fall into this category is not correct. The vast majority of accounts on the list compiled by the examiner, exist because the employees have email accounts. EVERY fulltime Town of Grand Island employee has an active email address. Since the Town of Grand Island hosts its own [redacted] these employees also have restricted domain accounts. These employees, many of whom may be maintenance workers, may not utilize their Town email accounts. That does not preclude us from providing it. We also have (and continue to have need for) many Service and Vendor Service accounts, since we host most of our own software. The Vendor may not utilize the account for a period of time, if no updates are needed nor help desk calls are made. While we analyze user access periodically, we will review our User Access Procedures and make changes as appropriate.

See Note 2 Page 9

Respectfully yours,

Nathan McMurray

Appendix B: OSC Comments on the Town's Response

Note 1

The six computers are owned by the Town; five were in use at the time of our audit, and one was a new computer designated as a spare.

Note 2

Generally, users should only have access rights that are necessary to complete their job duties. Therefore, we question why employees or vendors need accounts if they are never used.

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 interviewed Town officials, employees and the IT Consultant to obtain an understanding of IT operations.
- We inquired about IT policies and procedures and reviewed written policies and procedures to obtain an understanding of controls over IT assets and operations.
- We compared the Town's master payroll list to user accounts enabled on the Town's network. We evaluated whether any users who were no longer employed by the Town still had active accounts in the Town's network. In addition, we reviewed user accounts that had not been accessed in six months or more.
- We used our professional judgment to select a sample of seven computers (from 81 computers in total), to examine and analyze the web browsing histories to determine whether employees were complying with the CUP. Our sample was based on risk and included computers used by employees with access to financial records, online banking and PPSI.
- We reviewed the IT Consultant's service call tickets and documentation to look for remote access requests during our audit period.
- We reviewed the IT Consultant's inventory to determine whether it was adequate and performed a physical inventory of computers on site to determine whether they were included.

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 GAGAS (generally accepted government auditing standards). 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.

Appendix D: 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

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

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

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