DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2018M-218

Town of Seneca Falls

Information Technology

MARCH 2019

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights **1**

Information Technology **2**

What Security Policies and Procedures Should the Board Adopt to Safeguard IT Data? 2

The Board Did Not Adopt IT Security Policies and Procedures 2

Officials Did Not Disable or Remove Unnecessary User Accounts . . 3

Why Should the Board Provide Security Awareness Training? 4

The Board Did Not Provide Security Awareness Training 4

Why Should the Town Maintain Hardware and Software Inventories? 4

Officials Did Not Maintain Comprehensive Hardware and Software Inventories 5

Why Should the Town Have a Disaster Recovery Plan? 5

The Town Does Not Have a Comprehensive Disaster Recovery Plan 6

What Do We Recommend? 6

Appendix A – Response From Town Officials **8**

Appendix B – Audit Methodology and Standards **9**

Appendix C – Resources and Services **10**

Report Highlights

Town of Seneca Falls

Audit Objective

Determine whether the Board established policies and procedures to adequately safeguard information technology (IT) assets.

Key Findings

The Board did not:

- Adopt IT policies and procedures to adequately address acceptable computer use, user access rights, disaster recovery, password security management, data breach notification and backups.
- Provide users with security awareness training to help ensure their understanding in security measures to protect the network.

Town officials did not:

- Ensure user accounts for former personnel were disabled or removed in a timely manner.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt policies and procedures to adequately address acceptable computer use, user access rights, disaster recovery, password security management, data breach notification and backups.
- Ensure the access rights for users no longer employed are revoked.
- Provide security awareness training to personnel who use IT resources.
- Address the IT recommendations communicated confidentially.

Background

The Town of Seneca Falls (Town) is located in Seneca County. The Town is governed by an elected five-member Town Board (Board), which is composed of four Board members and a Supervisor.

The Board is primarily responsible for the general management and oversight of operations. The Town uses a variety of electronic data and computer resources in daily operations, including those related to finances, the Justice Court and Police Department.

Quick Facts	
Population	9,000
Total Employees (including Part-time and Seasonal)	160
IT User Accounts	74

Audit Period

January 1, 2017 – June 19, 2018

Information Technology

The Town uses IT to initiate, process, record and report transactions. It also relies on IT systems for Internet access, email and maintaining financial information. Before the end of 2017, the Town contracted with an IT consultant to manage the network as needed, and has since hired a full-time Network Administrator. The Network Administrator is responsible for various IT related tasks such as setting up new computers, network access and trouble-shooting network problems. If IT systems are compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair.

What Security Policies and Procedures Should the Board Adopt to Safeguard IT Data?

The board should adopt a computer policy that defines acceptable use. An effective process for safeguarding the IT system includes an acceptable computer use policy that holds users accountable for properly using and protecting resources and defines the procedures for computer, Internet and email use.

Additionally, the board should adopt policies and procedures for granting, revoking, modifying and monitoring individual access rights and a process to monitor and review these rights once granted. To ensure the highest level of security over town data, the board should also adopt policies and procedures for security management. All IT policies and procedures should be periodically reviewed and updated to reflect changes in technology and the computing environment.

The Board Did Not Adopt IT Security Policies and Procedures

The Board did not adopt adequate policies and procedures for monitoring acceptable computer use and granting, revoking, modifying and monitoring individual access rights to the networks. In addition, the Board did not adopt a comprehensive disaster recovery plan or policies and procedures for password security management, data breach notification and backups.

Town officials have an acceptable use policy, which is included in the employee handbook. However, employees and officials were generally unaware of the policy’s existence and not required to sign a statement to acknowledge that they are aware of this policy.

Although sufficient Town-wide IT policies were not in place, the Police Department (Department) established policies for internal computer and electronic messaging (acceptable use) and continuity of operations (a disaster recovery plan) specific to Department operations. Further, Department officials require all employees to sign an acknowledgment form for each of these policies.

We performed testing during our audit fieldwork in January and February 2018 and reviewed 17 of the Town's 61 computers.[1] We found that on 13 computers, employees accessed questionable websites including the following: gaming, shopping, social media, travel and job search.

Because users were able to access questionable websites and local user accounts were left enabled when individuals were no longer employed, there is a significantly increased risk that the Town could lose important data, suffer a serious interruption in operations and unauthorized individuals could access computerized data to copy, manipulate or delete sensitive information.

Further, without policies that specify appropriate computer use and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities and may not be able to notify individuals in a timely manner in the event that their private information was accessed.

Officials Did Not Disable or Remove Unnecessary User Accounts

The Board did not implement a process to address deactivating unnecessary user accounts. As a result of our testing (in January and February 2018), we found that 19 (26 percent) of the 74 network user accounts had not been used to logon to a computer in at least six months and five accounts (7 percent) were for individuals no longer employed. Because these accounts are still enabled and passwords are typically not set to expire, these accounts can still be used to logon to the network.

Additionally, unnecessary local user accounts[2] are enabled on two of the five servers and 13 of 17 computers reviewed. Specifically, 73 of the 88 local user accounts we identified have not been used to logon to the respective computer or server in at least six months, 35 of these accounts (40 percent) have never been used and five accounts (6 percent) were for individuals who were no longer employed.

Furthermore, because generic accounts[3] are used Town officials can be prevented from tracing suspicious activity to a specific individual, presenting difficulties in holding the responsible user accountable for their actions. Our examination identified 32 generic accounts (i.e., assessor, clerk, chief, guest and administrator) on the network of which seven were unnecessary.

[1] Refer to Appendix B for information on our sampling methodology.

[2] A local user account is one whose username and encrypted password are assigned to a specific computer.

[3] 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.

Any unnecessary accounts should be disabled or removed as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete personal, private, and sensitive information (PPSI). Of particular risk are the accounts of former employees, because these accounts could potentially be used by those individuals for malicious activities. These accounts create additional work to manage access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

Why Should the Board Provide Security Awareness Training?

Computer users need to be made aware of security risks and trained in practices that reduce internal and external threats to IT systems and data. While IT policies provide guidance for computer users, cybersecurity training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on:

- Emerging trends in information theft and other social engineering reminders.
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet.
- Password controls.
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed.
- Restricting physical access to IT systems and resources.
- Protecting IT systems from intentional or unintentional harm, loss or compromise.

The Board Did Not Provide Security Awareness Training

The Board did not provide employees with security awareness training to help ensure they understand security measures necessary to protect the network. As a result, employees may not be aware of risks and inadvertently expose the Town's IT assets to cybersecurity attacks, loss and misuse.

Why Should the Town Maintain Hardware and Software Inventories?

To safeguard assets and data, it is essential that town officials appropriately manage hardware and software, including licenses. Therefore, officials must have an understanding of the hardware and software used and ensure licensing compliance. Inventory records should include an item's description including version and serial number, a description of the physical location or the computer on which any software is installed and any pertinent licensing information.

Knowing what hardware and software is used allows town officials to better manage software by ensuring that patches[4] are up-to-date and that only appropriate software is used, reducing the risk of unwanted consequences and unnecessary costs that could result from using unauthorized software.

Officials Did Not Maintain Comprehensive Hardware and Software Inventories

Although we found that Police Department officials maintained hardware and software inventory records for their Department, Town officials did not maintain a comprehensive Town-wide inventory list of hardware and software. As a result, the Board cannot ensure that all hardware is properly accounted for, and that the software programs are properly licensed and for legitimate purposes.

In January 2018, Town officials became aware that a computer, which contained their electronic door controller software, was missing and later found that it was taken by the prior IT consultant.[5] Town officials were informed that this computer was owned by the consultant, but were unable to verify this because their inventory list was inadequate.[6]

Ultimately, officials determined that this computer was not Town property, but only after extensive research and additional records review. Had Town officials maintained a comprehensive hardware inventory, it would have been clear that this particular IT equipment was not owned by the Town, and the risk of loss, misuse or abuse of assets would have been reduced. As of the end of our audit fieldwork, comprehensive inventories were still not developed.

Further, outdated and unauthorized software applications not only provide additional opportunities for malicious attacks but also indicate a lack of productivity if employees use these applications during the workday.

Why Should the Town Have a Disaster Recovery Plan?

The board should adopt a disaster recovery plan to describe how town officials will deal with potential disasters that affect the IT system. A disaster recovery plan provides a framework for reconstructing vital operations to ensure that time-sensitive operations and services can be resumed in the event of a disaster.

[4] Patches update software programs with important information that could potentially protect systems running those programs from attacks. A patch can be an upgrade (adding features), computer bug fix, new hardware driver installation or an update to address new issues, such as security or stability problems.

[5] This consultant was contracted with to provide IT services to the Town through December 31, 2017 and was subsequently replaced by the full-time Network Administrator hired on December 11, 2017.

[6] As a result, the Town lost most access to its electronic door control system for several weeks, ultimately needing to purchase a new computer and contact the vendor to reinstall the appropriate software and command codes. In the meantime, most doors could be opened only with physical keys.

Disasters may include any sudden, unplanned catastrophic event (e.g., fire, computer virus or inadvertent employee action) that compromises the availability or integrity of the IT system and data.

Typically, a disaster recovery plan involves an analysis of business processes and continuity needs, a focus on disaster prevention, the roles of key individuals and the precautions to maintain or quickly resume operations. Additionally, the disaster recovery plan should include data backup procedures and periodic testing of the backups to ensure they will function as expected. The plan should be distributed to all responsible parties, periodically tested and updated as needed.

The Town Does Not Have a Comprehensive Disaster Recovery Plan

The Board did not develop a disaster recovery plan to address potential disasters and the continuity of operations, including IT. While the Police Department established an internal continuity of operations plan specific to Department operations, Town officials did not establish a comprehensive plan encompassing all Town operations and departments.

Consequently, in the event of a disaster, officials have no guidance to minimize or prevent the loss of equipment and data or to appropriately recover data. Without a disaster recovery plan, the Town could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

What Do We Recommend?

The Board should:

1. Adopt adequate, written IT policies and procedures to address acceptable computer use, individual access rights, backups, password security management, data breach notification and disaster recovery.

2. Periodically review and update all IT policies and procedures to reflect changes in technology and the computing environment. Verify that IT back-up procedures are functioning properly.

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

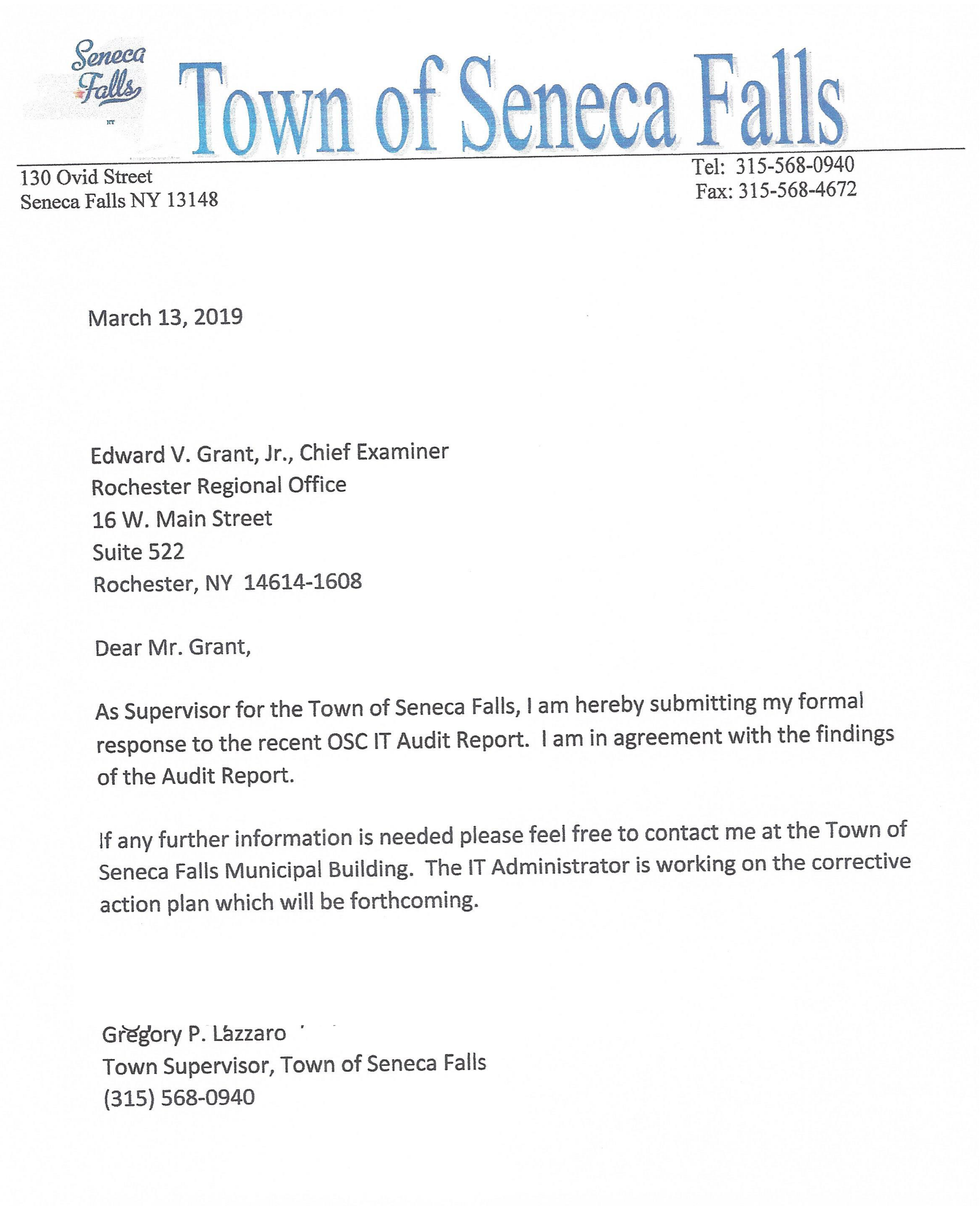
The Network Administrator should:

4. Evaluate all existing network and local user accounts and remove or disable any deemed unnecessary. Accounts should be periodically reviewed to determine whether they are appropriate and necessary.

5. Develop and maintain complete, comprehensive hardware and software inventories, which include adequate information to appropriately identify equipment and the total number of licenses owned.

6. Monitor computer use to ensure that only approved and/or appropriate software is installed.

Appendix A: Response From Town Officials



Town of Seneca Falls

130 Ovid Street
Seneca Falls NY 13148

Tel: 315-568-0940
Fax: 315-568-4672

March 13, 2019

Edward V. Grant, Jr., Chief Examiner
Rochester Regional Office
16 W. Main Street
Suite 522
Rochester, NY 14614-1608

Dear Mr. Grant,

As Supervisor for the Town of Seneca Falls, I am hereby submitting my formal response to the recent OSC IT Audit Report. I am in agreement with the findings of the Audit Report.

If any further information is needed please feel free to contact me at the Town of Seneca Falls Municipal Building. The IT Administrator is working on the corrective action plan which will be forthcoming.

Gregory P. Lazzaro
Town Supervisor, Town of Seneca Falls
(315) 568-0940

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 obtained and reviewed the Town's IT policies and procedures.
- We interviewed Town officials to gain an understanding of the Town's IT environment and internal controls.
- We visited all Town locations to determine an inventory of Town-owned computers, based on physical observation of those computers in operation. We randomly selected 17 of 61 computers to run a specialized computer audit tool and analyzed reports obtained. We used the tool to identify installed software and updates, local account password settings and user account configurations. We also reviewed the Internet web histories to determine if the computers were being used for appropriate activities.
- We ran specialized audit scripts and network scanners on the Town's five servers to identify certain vulnerabilities related to the system.

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 relevant population size 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 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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

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

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