REPORT OF EXAMINATION | 2021M-158

Town of Hempstead

IT Access Controls

AUGUST 2022

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

Contents

Report Highlights

Town of Hempstead

Audit Objective

Determine whether Town of Hempstead (Town) officials established adequate access controls to help safeguard Town information technology (IT) systems against unauthorized access.

Key Findings

Town officials did not establish adequate access controls to help safeguard IT systems against unauthorized access. The Board and Town officials did not:

- Develop and adopt comprehensive IT policies and procedures addressing key IT security issues, such as breach notification, and those related to acceptable computer use, protection of PPSI, application and network controls, password security, and user access controls.
- Provide IT security awareness training to all IT users, so they understand IT security measures and their roles in safeguarding data and IT assets.

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

Key Recommendations

The Board should:

- Adopt comprehensive IT security policies and procedures, and periodically review them.
- Provide periodic IT security awareness training.

District officials agreed with our recommendations and indicated that they were in the process of implementing corrective action.

Background

The Town is located in Nassau County. The Town provides general government support to its residents.

The Town is governed by an elected seven-member Town Board (Board), which is composed of six Council members and the Town Supervisor. The Board is responsible for the general oversight of the Town's operations and finances.

The Town relies on its IT systems for internet access, email, maintaining financial data, and accounting and reporting for many services that the Town provides. The Town's IT Commissioner is responsible for oversight of the IT department and systems.

Quick Facts

Full Time Employees	1,906
Network User Accounts	1,149

Audit Period

January 1, 2018 - March 31, 2020, but extended our audit period to October 21, 2021 to obtain updated records.

IT Access Controls

What Policies and Procedures Should the Board Adopt to Help Safeguard Access to Town IT Systems?

IT security policies describe the tools and procedures used to help protect IT systems, including data and networked applications, such as email backup systems, and help to define a board's expectation for appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the board to adopt security policies for key IT security issues to help safeguard against unauthorized access, use or loss.

The board should adopt computer policies that take into account people, processes and technology and communicate them to all users of the IT assets.[1] New York State Technology Law[2] requires municipalities to have a breach notification policy that requires certain individuals to be notified when there is a system security breach involving private information. In addition, the board should have acceptable computer use policies that address security awareness and define specific consequences for violations.

Some networked applications, such as email backup systems, may inherently provide access to private, personal or sensitive information (PPSI). Properly designed and written procedures help to ensure access and use of the email backup system is authorized, appropriate and documented. Access should be limited to only authorized officials so that PPSI is safeguarded. Each user should have and use their own user access account to ensure accountability. When multiple users are allowed to share user access accounts, activity in the email backup system may not be able to be traced back to a single user. Additionally, application logs from the email backup system should be reviewed periodically to ensure actions are properly authorized. Any unusual or unauthorized activity could indicate a breakdown in controls or possible misuse or abuse.

Policies directing officials help to protect PPSI, provide for appropriate management of the networked applications and develop strong password and user access controls, are essential for effective IT governance.

The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring compliance with IT policies.

1 Refer to our publication Information Technology Governance available at http://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

2 New York State Technology Law, Section 208

The Board Did Not Adopt IT Security Policies and Procedures

The Board did not adopt IT security policies and procedures addressing key IT security issues, such as breach notification, and those related to acceptable computer use, protection of PPSI, application and network controls, password security, and user access controls. Therefore, the Board did not provide guidance to officials and employees necessary to help safeguard Town IT systems. Consequently, IT assets are at risk for unauthorized access and loss and the Town could incur a potentially costly disruption of operations and services.

…[T]he Board did not provide guidance to officials and employees necessary to help safeguard Town IT systems.

The Town's IT Commissioner is responsible for oversight of the IT department and the Town's IT systems. This oversight includes advising the Board on policies and implementing procedures to help ensure that IT systems are safeguarded. The Town's IT department distributed written guidance regarding Internet, Email, and connected devices to users of the Town's IT systems. The guidance states that the use of devices on the Town's computer network should be restricted to Town issued devices, used for official Town business only and advises the reader of consequences for violating the policy. However, since this policy was not adopted by Board resolution, it may not carry the Board's authority when it is necessary to enforce consequences of violation. The pandemic impacted access to Town facilities and officials, resulting in a temporary suspension of fieldwork. As of the end of our fieldwork in October 2021, the Commissioner acknowledged the Board had not adopted these IT security policies.

While comprehensive policies will not guarantee the safety of IT systems, the failure to adopt appropriate policies significantly increases the risk 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. Further, without properly designed and functioning procedures to safeguard PPSI, there is an increased likelihood that significant errors or fraud could occur and remain undetected. In addition, without a breach notification policy, officials may not understand or be prepared to fulfill their legal obligation to notify affected individuals should a breach occur.

Town Officials Did Not Develop Written Procedures for the Access and Use of the Email Backup System

Town officials employ the use of an email backup system for the purpose of retaining emails. Per the IT Commissioner, the system is only accessed to obtain information for a Freedom of Information Law (FOIL)[3] request or a Town investigation. However, officials have not developed written policies

3 The Freedom of Information Law (Public Officers Law, Article 6) (FOIL) grants members of the public access to the records of government in accordance with its provisions.

and procedures to help ensure the access and use of this system is properly authorized. As a result, searches within the system are performed by employees in the Town's IT department without adequate oversight.

The IT department did not maintain documentation authorizing searches, including the purpose, who requested the search, who authorized the search and the employee who performed the search. We reviewed access logs generated by the email backup system for our audit period to determine if logged events represented appropriate and authorized use of the system. Although Town officials informed us that the selected activities were each pursuant to a FOIL request or internal investigations, the IT department was unable to substantiate those activities with adequate documentation. In addition, a significant portion of these tasks were completed by IT system administrators while accessing the system using a shared user account.

During our audit period, there were 255 separate logins by the shared user account. The use of a shared user account limits accountability of IT system administrators because officials may not be able to identify the individual who performed the activity. Town officials disabled this account in January 2020 so the shared account could no longer be used.

The IT Commissioner informed us that IT system administrators began keeping a log of tasks performed within the email backup system in November 2018. The logs contained a date, time, and partial sentence reason. However, the logs do not clearly detail the purpose for accessing the system, the tasks performed, which IT system administrator performed the tasks, and who authorized the tasks. As a result, the IT Commissioner may still be unable to determine whether actions performed by IT system administrators were appropriate or an authorized use of the system. In October 2021, the IT Commissioner stated that he is reviewing the IT administrator's log every six months. This is not an effective procedure because the logs do not contain sufficient information and he is not reconciling the activity log prepared by IT system administrators with the access logs generated by the system.

Without adequate policies and procedures over the use and access of the email backup system, activity could occur that is unauthorized, inappropriate, and undocumented, whether inadvertently due to the lack of awareness and clear expectations or otherwise. Given the potential for PPSI being sent in an email, adequate controls are necessary to help ensure security over PPSI is not compromised.

The use of a shared user account limits accountability of IT system administrators because officials may not be able to identify the individual who performed the activity.

How Can IT Security Awareness Training Help Town Officials Safeguard Access to Town IT Systems?

To minimize the risk of unauthorized access, use and/or loss of data and PPSI, town officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and the town's IT resources, systems, and data. In addition, the training should communicate the town's related policies and procedures to all users, so they understand IT security measures and their roles in safeguarding data and IT assets.

The training could center on emerging trends such as information theft, social engineering attacks,[4] 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 information that attendees need to perform their jobs, such as securing user access and PPSI.

The training could 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; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

> …[T]raining should communicate the Town's related policies and procedures to all users, so they understand IT security measures and their roles in safeguarding data and IT assets.

Town Officials Did Not Provide IT Security Awareness Training

Town officials did not provide IT users with IT security awareness training to communicate key IT security policies and procedures to help ensure the users understood IT security measures designed to safeguard IT systems from unauthorized access, use and loss. Accordingly, Town officials cannot be assured that there is adequate protection of the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Officials were not aware that this training was necessary to help safeguard the Town's IT systems. Without IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise the Town's IT systems and security. As of the end of our fieldwork in October 2021, the IT Commissioner acknowledged this training had not been provided. As a result, Town financial data and PPSI could be at a greater risk for unauthorized access, use or loss.

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

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies and procedures addressing key IT security issues such as breach notification, acceptable computer use, protection of PPSI, application and network controls, password security and user access controls.

2. Periodically review and update policies and procedures to reflect changes in technology and the Town's computing environment.

3. Ensure proper oversight of the email backup system is provided, including written procedures and periodic review of the system access logs to ensure that all access is authorized and appropriate.

The IT Commissioner should:

4. Implement procedures to ensure that access to the email backup system is properly authorized, appropriate and documented.

5. Periodically review email backup system application logs to ensure usage is authorized and appropriate.

6. Ensure IT policies are communicated to employees.

7. Ensure IT security awareness training is periodically provided to users of the Town IT system.

Appendix A: Response From Town Officials

Town of Hempstead

The Department of
Information and Technology
1WASHINGTON STREET,
HEMPSTEAD, N.Y. 11550-4087
(516) 489-5000 FAX# (516) 489-1571

DONALD X. CLAVIN Jr.,
Supervisor

August 2, 2022

Mr. Ira McCracken
Office of the State Comptroller
250 Veterans Memorial Highway
Hauppauge, New York 11788

Dear Mr. McCracken,

This Office, in conjunction with The Town's Office of the Comptroller have reviewed the Draft Report of Examination of the Town of Hempstead's Information and Technology Access Controls for the period spanning from 2018-2019 (hereinafter referred to as "the Report"). Please accept this letter as the Town's collective and official RESPONSE AND CORRECTIVE ACTION PLAN to the aforementioned Report.

IT Access Controls

As a general point of reference, Section 54-1 of the Town Code established the Department of Information and Technology by the Town Board. Section 54-1 delegates the power and confers the responsibility to the Commissioner of the Department to create policies and procedures to safeguard private, personal, or sensitive information (PPSI). See Section 54-1. The Commissioner has in fact created such policies and instituted them to safeguard PPSI and protect IT systems, including but not limited to, data and networked applications, such as backup systems. All users are familiar with Town policies with respect to the use of Town systems and safeguarding said systems against unauthorized access, use or loss. Each employee, upon hire must sign the acknowledgement forms of the Department's policies.

We appreciate your comments that the Policies and Procedures should be adopted by the Town Board and as such we are currently working on refining our policies that address the security of PPSI, breach notification, access, penalties for violations, and proper logging of our backup emails, as well as reconciliation of email back-up access-and-requests for presentation to the Town Board for approval and passage.

We appreciate your comments regarding our email back-up systems procedures that were in effect during the reporting years 2018-2019, however, since 2020 the Town has implemented the following measures to mitigate the concerns raised in the Report:

- The email back-up system shared user accounts are disabled and only three people in our Systems Group have access under unique, identifiable user IDs. The email back-up system allows only three people in our systems group access under unique, identifiable user ID's. The systems group has done away with shared user accounts back in 2019.
- The Department is continuously looking to improve upon our IT Security Awareness Training by utilizing different methods to educate Town Employees on how to safeguard the Town's systems and equipment. For example, we have provided informative e-mails to all employees explaining the importance of not opening up foreign emails from unknown users, not clicking on any links, and also not sharing their usernames and passwords with other users. Currently, the Town is also conducting phishing tests to further educate users who click on anything they are not supposed to. The Town will continue to implement various training to further enhance the Security of its Systems.

In closing, we appreciate the time and effort you dedicated in your audit of the Town's IT infrastructure as it stood in the years 2018-2019. As noted in our response, the Town has implemented many new procedures and programs that have alleviated most of the concerns highlighted in the Report. For those recommendations you have provided that have not already been implemented, we look forward to fully reviewing them and implementing them, where applicable.

Sincerely,

Arthur R. Primm, Jr.
Commissioner of Information and Technology

ARP/vc

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 interviewed Town officials and reviewed Board minutes, resolutions, and Town policies and procedures to gain an understanding about how the Town safeguards its IT systems against unauthorized access, use and loss.
- We used a computerized audit script which we ran on March 12, 2020 to examine the Town's domain controller and analyzed the data produced to assess the necessity and appropriateness of network user accounts and security settings. We reviewed 1,149 enabled network user accounts to determine whether IT officials adequately managed user accounts and established strong controls over user access.
- We also compared these 1,149 network user accounts with the Town's payroll to determine whether users were currently employed by the Town.
- We used our professional judgment to select a sample of 23 Town computers to include employees whose job duties included routinely accessing PPSI, and employees in various departments in the Town Hall. We ran a computerized audit script on March 12, 2020 on these computers to identify and assess installed software, local user account and security settings.
- We interviewed officials and reviewed access logs for the Town's email backup system for our audit period to assess whether the access was authorized and appropriate.
- We judgmentally selected a sample of 15 logged events from the email backup system access logs to determine if the events were properly authorized, appropriate, and documented.

Our audit also examined the adequacy of certain information technology 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.

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 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/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

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

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/local-government

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties

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