

# Town of Lansing

## Information Technology

JULY 2022



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

# Contents

---

- Report Highlights . . . . . 1**
  
- Information Technology . . . . . 2**
  - How Should Town Officials Manage Network User Accounts? . . . . 2
  - Town Officials Did Not Properly Manage Network User Accounts . . . 2
  - What Policies and Procedures Should a Board Adopt to Safeguard IT Assets and Data? . . . . . 3
  - The Board Does Not Have Adequate IT Policies or Require IT Security Awareness Training. . . . . 3
  - What Do We Recommend? . . . . . 4
  
- Appendix A – Response From Town Officials . . . . . 5**
  
- Appendix B – Audit Methodology and Standards . . . . . 6**
  
- Appendix C – Resources and Services . . . . . 7**

# Report Highlights

## Town of Lansing

### Audit Objective

Determine whether Town of Lansing (Town) officials ensured information technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

### Key Findings

Town officials did not ensure IT systems were adequately secured and protected against unauthorized use, access and loss. In addition to sensitive IT control weaknesses that we communicated confidentially to Town officials, we found:

- The Town had seven unneeded network user accounts.
- The Town Board (Board) did not create adequate written IT policies for network user access, online banking and breach notification.
- The Board did not require IT security awareness training for computer users.

### Key Recommendations

- Review user access on a routine basis and disable unnecessary network user accounts in a timely manner.
- Develop and adopt adequate written IT policies.
- Require periodic IT security awareness training for personnel who use Town IT resources.

Town officials generally agreed with our findings and recommendations and indicated they planned to take corrective action.

### Background

The Town is located in Tompkins County and includes the Village of Lansing.

The Town is governed by an elected Board composed of the Town Supervisor (Supervisor) and four Board members. The Board is responsible for the general management of Town operations, which includes establishing policies and procedures to help protect IT systems and provide a secure IT environment.

The Supervisor is responsible for the Town's day-to-day activities, including managing IT assets. The Parks and Recreation Supervisor is responsible for the overall management of the Town's IT infrastructure, with the assistance of the Town's IT vendor.

#### Quick Facts

Computers	39
Employees	87
Network User Accounts	36

### Audit Period

January 1, 2020 – January 20, 2022

# Information Technology

---

## How Should Town Officials Manage Network User Accounts?

Network user accounts provide users with access to town network resources and should be actively managed to help safeguard computerized data. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI),<sup>1</sup> make changes to employee records or deny access to computerized data.

A town should have written policies and procedures for granting, changing and disabling user access and permissions to the network. To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions, including their creation, use and dormancy and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer used or needed, they should be disabled in a timely manner.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Towns should limit the number of generic user accounts, and officials should routinely evaluate and disable any generic accounts that are not related to a specific need.

## Town Officials Did Not Properly Manage Network User Accounts

The Board and Town officials did not adopt written IT policies and procedures for managing network user accounts and permissions. The Parks and Recreation Supervisor, with the assistance of the Town's IT vendor, managed and maintained the Town's network access. Department heads verbally conveyed modifications of network user accounts to the Parks and Recreation Supervisor. The Parks and Recreation Supervisor told us he was immediately aware of when to terminate employee access to the network because of the limited number of Town employees.

We reviewed the Town's 36 enabled network user accounts, and determined that seven network user accounts (19 percent) were unneeded and could be disabled, including:

---

<sup>1</sup> PPSI is any information that 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.

- 
- Three generic user accounts,
  - Three user accounts of former employees, and
  - One former official's user account.

The three generic accounts were not used in over six months and the Parks and Recreation Supervisor determined they could be disabled. The Parks and Recreation Supervisor told us the former employees' network user accounts were not disabled because he believed current employees needed access to the accounts for operations. Additionally, the Parks and Recreation Supervisor attempted to disable one unneeded former employee account but was unaware the account remained enabled.

Unneeded network user accounts can be potential entry points for attackers and used to inappropriately access and view PPSI. This increases the risk that data could be changed intentionally or unintentionally, or used inappropriately.

### **What Policies and Procedures Should a Board Adopt to Safeguard IT Assets and Data?**

A board should adopt written IT policies to protect PPSI from unauthorized access. To ensure the highest level of security over town data, the board should adopt written IT policies for security management, including a policy for online banking. Also, New York State Technology Law Section 208 requires towns to have a breach notification policy that details actions to be taken to notify affected individuals if PPSI is compromised. All IT policies should be periodically reviewed and updated to reflect changes in technology and the computing environment.

Computer users need to be aware of security risks and be 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 users understand their roles and responsibilities, and provides them with the necessary skills to perform them. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything needed to perform their jobs. IT security awareness training should reinforce IT policies and focus on security in general or a narrow aspect of security (e.g., the dangers of opening an unknown email or attachment or downloading files from the Internet).

### **The Board Does Not Have Adequate IT Policies or Require IT Security Awareness Training**

The Board did not adopt adequate written IT security management policies, including policies for online banking and breach notification. The Board also did not require IT security awareness training for employees using Town computers to help ensure they understand security measures to protect IT assets.

---

The Supervisor told us IT security management policies were not established because the Board leaves IT-related matters to the Parks and Recreation Supervisor, and the Supervisor was unaware of the requirement to have a breach notification policy. The Parks and Recreation Supervisor told us an IT security awareness training link was provided to employees in the past; however, he could not locate a record of the email and did not monitor whether employees completed the training. Ultimately, the Board and Town officials are responsible for ensuring that Town assets are properly secured and safeguarded and appropriate policies and procedures are developed and adopted.

While policies will not guarantee the safety of IT assets and data, not adopting adequate policies and requiring IT security awareness training significantly increases the risk that users will not understand their responsibilities and are more likely to be unaware of situations that could put Town data and PPSI at greater risk for unauthorized access, misuse and loss. An online banking policy outlines procedures to follow when responding to potentially fraudulent activity. Further, without a breach notification policy, the Town is not fulfilling its legal obligation to have a policy to notify affected individuals in a timely manner in the event their private information was accessed.

### **What Do We Recommend?**

The Board should:

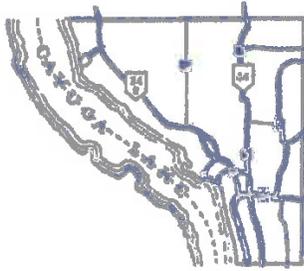
1. Adopt written IT policies to address network user access, online banking and breach notification, and periodically review the policies and update them as needed.
2. Require IT security awareness training for employees who use IT resources.

The Parks and Recreation Supervisor should:

3. Routinely review network user accounts and ensure that unneeded user accounts are disabled in a timely manner.

# Appendix A: Response From Town Officials

---



## **TOWN of LANSING**

*"Home of Industry, Agriculture and Scenic Beauty"*

PO Box 186  
29 Auburn Road  
Lansing, NY 14882

June 22, 2022

Office of the State Comptroller  
Binghamton Regional Office  
44 Hawley Street - Suite 1702  
Binghamton, NY 13901-4417

The Town of Lansing is in receipt of the Draft Audit Report, Information Technology for the period of January 1, 2020 – January 20, 2022. On behalf of the Town of Lansing, we would like to thank your team for their professionalism and courtesy during our recent audit. We would like to point out that scope of the audit period coincides with the Covid-19 pandemic, during this time our IT support was navigating many employees through working from home during those challenging times. The Town is extremely proud of their internal IT as well as outside IT support company's efforts during these unprecedented times.

The priority of the Town of Lansing is to ensure consistency and fiscal responsibility for the services provided to our taxpayers while safeguarding all our community's resources. We take our responsibility to this community very seriously and appreciate the opportunity to continually improve our policies and procedures.

For each recommendation included in the draft audit report we plan to submit a corrective action plan as soon as possible, although we have already begun making changes and have corrected several of the findings already. The Town Board will be making policy and procedure changes to its employee handbook later this year when it will be updated by an outside agency. The Town will utilize the recommendations from the draft audit report to further strengthen our IT environment.

In closing, I would like to again thank you for the professionalism of your staff and the opportunity to have clear and specific guidance on what the Town needs to address.

Sincerely,

Mr. Edward J. LaVigne  
Town of Lansing Supervisor

## 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 IT policies and procedures and interviewed Town officials to gain an understanding of the Town's IT operations and determine the adequacy of the policies and procedures.
- We reviewed the Town's network user accounts and related settings using a computerized audit script that we ran on January 20, 2022. We compared these 36 network user accounts to the active employee list and discussed these user accounts with Town officials to identify inactive and unneeded user accounts.
- We reviewed available documentation and made inquiries of Town officials to determine whether IT security awareness training was required for users of IT resources.

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.

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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](mailto:localgov@osc.ny.gov)

[www.osc.state.ny.us/local-government](http://www.osc.state.ny.us/local-government)

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

---

**BINGHAMTON REGIONAL OFFICE** – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: [Muni-Binghamton@osc.ny.gov](mailto:Muni-Binghamton@osc.ny.gov)

Serving: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga,  
Tompkins counties



Like us on Facebook at [facebook.com/nyscomptroller](https://facebook.com/nyscomptroller)

Follow us on Twitter [@nyscomptroller](https://twitter.com/nyscomptroller)