DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-4

Town of Urbana

Access Controls

MAY 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Town of Urbana

Audit Objective

Determine whether Town of Urbana (Town) officials properly configured network and computer user access controls to safeguard the Town’s IT systems.

Key Findings

Town officials (officials) did not adequately configure network and computer user access controls. In addition to sensitive IT control weaknesses that were communicated confidentially to officials, officials did not:

- Adopt comprehensive written information technology (IT) policies and procedures addressing areas key to securing user access controls to minimize the risk of data loss.
- Provide IT security awareness training.
- Adequately manage network and local user accounts and permissions.
- Enter into an adequate service level agreement (SLA) with the Town’s IT vendor or monitor compliance with this agreement

Key Recommendations

- Adopt comprehensive written IT security policies and procedures and ensure computer users receive comprehensive IT security awareness training.
- Regularly review and update user accounts and permissions and disable those that are unnecessary.
- Establish a detailed, clear and comprehensive SLA with the IT vendor to address the Town’s specific needs and expectations and the roles and responsibilities of all parties.

Background

The Town, located in Steuben County, is governed by an elected Town Board (Board), composed of a Supervisor and four Board members.

The Board is responsible for the general oversight of operations and finances including establishing IT policies and procedures to help secure user access.

Town employees and officials use and rely on the Town’s IT assets and systems to initiate, process, record and report transactions, email and for Internet access.

The Town contracts with an IT vendor to service the Town’s network and computers per a quarterly maintenance agreement.

Quick Facts	
Employees/Officials	17
Computers	14
Tested	8
User Accounts	
Network (Enabled)	9
Tested	9
Local (on 8 Tested Computers)	22
Tested	22

Audit Period

January 1, 2020 – December 17, 2021

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

Access Controls

How Should a Board Secure Network and Computer User Access?

IT security policies describe the tools and procedures used to help protect data and information systems, define a board's expectations for appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential that a board establish comprehensive written policies for IT areas key to securing network and computer user access such as acceptable use, password security, computerized access controls, remote access, wireless network security, IT asset controls, physical security, incident response, breach notification[1] and online banking.

As it provides oversight and leadership for such policies, a board should take into account people, processes and technology. Subsequently, the board should periodically review these policies, update them as needed, designate personnel who are responsible for monitoring policy compliance and communicate the policies to all users.

Officials should develop written procedures for granting, changing and disabling user access to the town's network and computers. If officials choose to handle town official turnover by transferring user accounts from one official to the next, this should be done in accordance with a written transfer procedure. This procedure should ensure that the user account's password is changed immediately upon separation of the previous account user to prevent unauthorized activity, there are clear and documented end and start dates for each individual so there is no question who used the account at any given time, only one individual knows the current password, and that password changes do not follow a predictable pattern that would allow prior users to easily guess new passwords.

To minimize the risk of unauthorized access and misuse or loss of data and personal, private and sensitive information (PPSI),[2] officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all users. The training could center on emerging trends such as information theft, social engineering scams 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 information that attendees need to perform their job duties and responsibilities.

> ...[I]t is essential that a board establish comprehensive... policies for... acceptable use, password security, computerized access controls, remote access, wireless network security,... incident response, breach notification and online banking.

[1] New York State Technology Law Section 208 requires municipalities and other local agencies to have a breach notification policy that requires notification be given to certain individuals in the event of a system security breach, as it relates to private information.

[2] Personal, private or sensitive information (PPSI) is any information to which 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 or entities.

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; 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.

Lastly, to minimize the risk of unauthorized access, officials should actively manage network and computer user accounts and permissions, including their creation, use and dormancy and restrict users' access to applications, resources and data that are necessary for their day-to-day responsibilities. User accounts enable the system to recognize specific users and processes and allow system administrators to grant the appropriate access rights. When properly managed, user accounts also provide accountability by affiliating user accounts with specific users and processes and unneeded shared and generic user accounts are disabled.

Generally, local administrative accounts have oversight and control of computers, with the ability to add new users and change users' passwords and permissions. A local user with administrative permissions can make local computer changes, including installing programs of their own choosing and adjusting settings configured for security purposes. Officials should limit users with administrative permissions and regularly monitor all user access to ensure it is appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner.

The Board Did Not Establish Adequate IT Policies and Procedures

The Board has not adopted comprehensive written policies key to securing network and computer user account access, addressing computerized access controls, password security, remote access, wireless network security, IT asset controls, physical security, incident response, breach notification or online banking.

In addition, the Board-adopted acceptable use policy (AUP) lacks guidance on network and computer user access security. Even though the AUP requires advance approval prior to the user's installation and use of software or peripheral equipment and does not authorize personal use, officials indicated that users could connect personally owned devices to their computer without approval.

While comprehensive policies will not guarantee the safety of IT assets and data, not adopting adequate policies and procedures significantly 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. Further, without a breach notification policy, the Town is not in compliance with New York State Technology Law Section 208 and may not be able to fulfill its legal obligation to notify affected individuals that they should monitor their credit reports and bank activity if their private information was compromised.

The Board Did Not Ensure Users Had IT Security Awareness Training

The Board did not ensure users were provided with IT security awareness training to help ensure they understood IT security measures key to securing network and computer user account access.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. Officials cannot protect 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.

Without periodic, comprehensive IT security awareness training, users may not understand their responsibilities, are more likely to be unaware of a situation that could compromise network and computer user account access and the Board has no assurance users understand security measures to protect the Town's network and computerized assets. As a result, the Town's IT assets and PPSI are more vulnerable to loss and misuse. For example, users may not be prepared to recognize and appropriately handle malicious e-mail messages, which increases the risk of a ransomware or other type of malware infection on Town computers.

Officials Did Not Properly Manage Network and Computer User Accounts and Permissions

Because the Board did not implement comprehensive written policies and procedures for managing, limiting, securing and monitoring user access, officials were unaware of the need to properly manage network and computer (local) user accounts and permissions. As a result, shared network and local user accounts were not properly managed and unneeded network and local user accounts were not disabled on the network and user computers.

Town computers are networked, but the security settings are not centrally managed. Therefore, the security settings enforced for network and local user accounts are those configured on each individual server or user computer.

<u>Improper Transfer of User Accounts</u> – Town officials did not securely transfer shared network and local user accounts from departing to incoming officials.

Town officials did not establish written transfer procedures. Current officials stated that when they came into office they were provided the usernames and passwords to the prior officials' accounts. For example, we found the current deputy clerk is using the former deputy clerk's user account and password.

Network User Accounts – The network has nine enabled network user accounts, seven of which are shared accounts. Five shared network user accounts are assigned to specific Town offices, such as the clerk, constable, assessor, bookkeeper and code enforcement officer. We question the necessity of the constable account as it has never been used. The two remaining shared network user accounts are used by two individual IT vendor staff users.

Local User Accounts – Our review of eight Town computers identified 22 local user accounts consisting of 11 generic, nine shared and two assigned to individual users.

Fifteen of the 22 local user accounts were not used in at least six months. Unneeded local user accounts are additional entry points into a computer and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. When local user accounts are not used or monitored, compromised accounts may not be detected timely.

Unnecessary Administrative Permissions – Eighteen of the 22 local user accounts had administrative permissions on the eight computers tested. However, it is only necessary to have one local user account with administrative permissions on a computer to administer and maintain the computer. Therefore, 10 of the 18 accounts with administrative permissions are unneeded.

When users have unneeded administrative permissions to computers, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

Why Should the Board Establish an IT Contingency Plan?

An IT contingency plan is a town's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT disruption. An unexpected IT disruption could include inadvertent employee action, a power outage, software failure caused by a virus or other type of malicious software, equipment destruction or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such an event.

The content and length of and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the town's operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to enable the recovery of an IT system and/or electronic data as quickly and effectively as possible following an unplanned disruption which could significantly reduce the resulting impact.

Because IT often supports key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining a town's critical business processes in the event of a disruption. The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity.

The IT contingency plan can also include, among other items deemed necessary by the town, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Communication protocols with outside parties,
- Prioritized mission critical processes,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,
- Backup methods and storage policies, and
- Details concerning how the plan will be periodically tested.

The Board Did Not Establish an IT Contingency Plan

The Board did not establish a comprehensive IT contingency plan to describe the procedures and technical measures officials would take to respond to potential disruptions and disasters affecting IT. Consequently, in the event of a disruption or a disaster, including a ransomware attack, there is no written guidance to follow to restore or resume essential operations in a timely manner and could help minimize damage and recovery costs.

Without a comprehensive plan, there is an increased risk that the Town could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Although Town officials told us that the financial data was backed up regularly, the backups were not tested periodically to ensure they functioned as expected.

Without periodic testing of backups, the Board cannot ensure the recovery of necessary data to continue operations if a security breach or system malfunction occurs. Without a viable plan, the Town is at risk of significant disruptions in business operations after a disastrous event and could suffer unnecessary and preventable losses.

How Can Officials Reduce the Risk of Inappropriate Online Banking Transactions?

Online banking provides a means of direct access to funds held in town bank accounts. Users can review current account balances and account information, including recent transactions, over the Internet and electronically transfer money between bank accounts and to external accounts. Because wire transfers of funds can involve significant amounts of money, the processing of town wire transfers must be controlled to help prevent unauthorized transfers from occurring. It is essential that officials authorize transfers before they are initiated and establish procedures to ensure that employees are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

To safeguard cash assets, a board must adopt written policies and procedures to properly monitor and control online banking transactions. A comprehensive written online banking policy clearly describes the online activities officials will engage in, specifies which employees are authorized to process transactions, and establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests. Officials must properly segregate the duties of employees granted access to the online banking applications to ensure that employees are unable to perform all financial transactions on their own. Segregation of duties should include monitoring bank accounts for unauthorized or suspicious activity frequently and regularly.

Good management practices require limiting the number of users authorized to execute online banking activities and the number of computers used. Banking agreements should identify current authorized users, and authorized online banking users should access bank accounts from authorized and properly secured computers. This could help minimize exposure to malicious software because the other computers are used for activities that may introduce additional risk to the computers' integrity, and transactions executed from those computers could be more at risk.

Town Officials Did Not Safeguard Online Banking Transactions

The Board did not adopt a written online banking policy that provided users a detailed approval process to verify the accuracy and legitimacy of online banking transactions. As a result, officials did not adequately segregate online banking duties and ensure authorized access to bank accounts was limited.

Officials also could not provide banking agreements for all bank accounts and the banking agreements provided were inadequate. The agreements did not outline how electronic or wire transfers should be accomplished, identify the names and numbers of the bank accounts from which transfers may be made, identify individuals authorized to request the transfer of funds or detail security procedures to verify payment orders or to detect errors in transmission or content of the payment order.

Without a sufficient written online banking policy and adequate agreements, officials cannot ensure that employees are aware of their responsibilities or that funds are being adequately safeguarded during online transactions. As a result, users could unintentionally expose online bank accounts to threats from malicious software and misappropriate funds without detection.

Due to these weaknesses, we reviewed all bank account transfers totaling $10,453,190 for the period January 1, 2018 through October 30, 2021 for appropriateness. We identified transfers totaling $430,530 to two unknown bank accounts. When we brought these to the Supervisor's attention, he contacted the bank which provided us with bank statements for these Town savings accounts that had a balance of $709,378 as of October 29, 2021.

Why Should a Board Establish a Service Level Agreement With Its IT Vendor?

A board should ensure that they have qualified IT personnel to manage the town's IT environment. This can be accomplished by using town employees, an IT vendor or both. To protect town assets and avoid potential misunderstandings, in addition to a contract with the IT vendor, a board should have a written service level agreement (SLA) with the town's IT vendor that clearly identifies the town's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI.

An SLA should establish comprehensive, measurable performance targets and remedies for not meeting those requirements so that there is a mutual understanding of the nature and required level of services to be provided. There should be no uncertainty about what services the contractor will deliver, when these services will be delivered and the cost. A vague agreement can lead to additional or increasing costs that were not expected or an underperformance of services needed to protect IT assets.

An SLA should provide detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement, scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The SLA should be reviewed by the town's legal counsel and IT staff, as appropriate. They should also be periodically reviewed, especially if the IT environment or needs change significantly. Developing a good SLA takes some effort but can help avoid potentially costly misunderstandings and establish an efficient and secure computing environment.

The Board Did Not Have an Adequate Service Level Agreement with the IT Vendor

Officials have relied on an IT vendor for IT services, technical assistance and purchase of IT equipment, as needed. The Board did not negotiate a specific written contract with the IT vendor, nor did officials enter into an SLA with the vendor to identify the specific services to be provided or the vendor's responsibilities. Instead, the Supervisor signed a generic three-year service maintenance agreement provided by the IT vendor.

The IT vendor provided assistance with, among other things, hardware and software issues, setting up new desktops and installing applications during visits. However, Town officials did not log or otherwise monitor the on-site visits or services provided to determine whether the expected visits were provided, or appropriate service fees were charged. The Town paid the IT vendor $8,968 during our audit period.

Further, the agreement with the Town's IT vendor is not adequate. It does not clearly state the Town's needs and expectations, nor does it establish measurable targets of performance so a common understanding of services can be achieved. The agreement does not define terminology, the scope of work to be performed or the impact of nonperformance. It does not establish limits, service level objectives, performance indicators, roles and responsibilities, security and audit procedures, billing and payment methodology.

Agreements that are not clear and comprehensive contribute to confusion over who is responsible for various aspects of the IT environment which ultimately puts the Town's IT resources at greater risk for unauthorized access, misuse or loss and can lead to additional costs or cost increases the Town is not expecting.

What Do We Recommend?

The Board should:

1. Adopt comprehensive written IT policies addressing IT areas key to securing network and computer user access to minimize the risk of data loss.

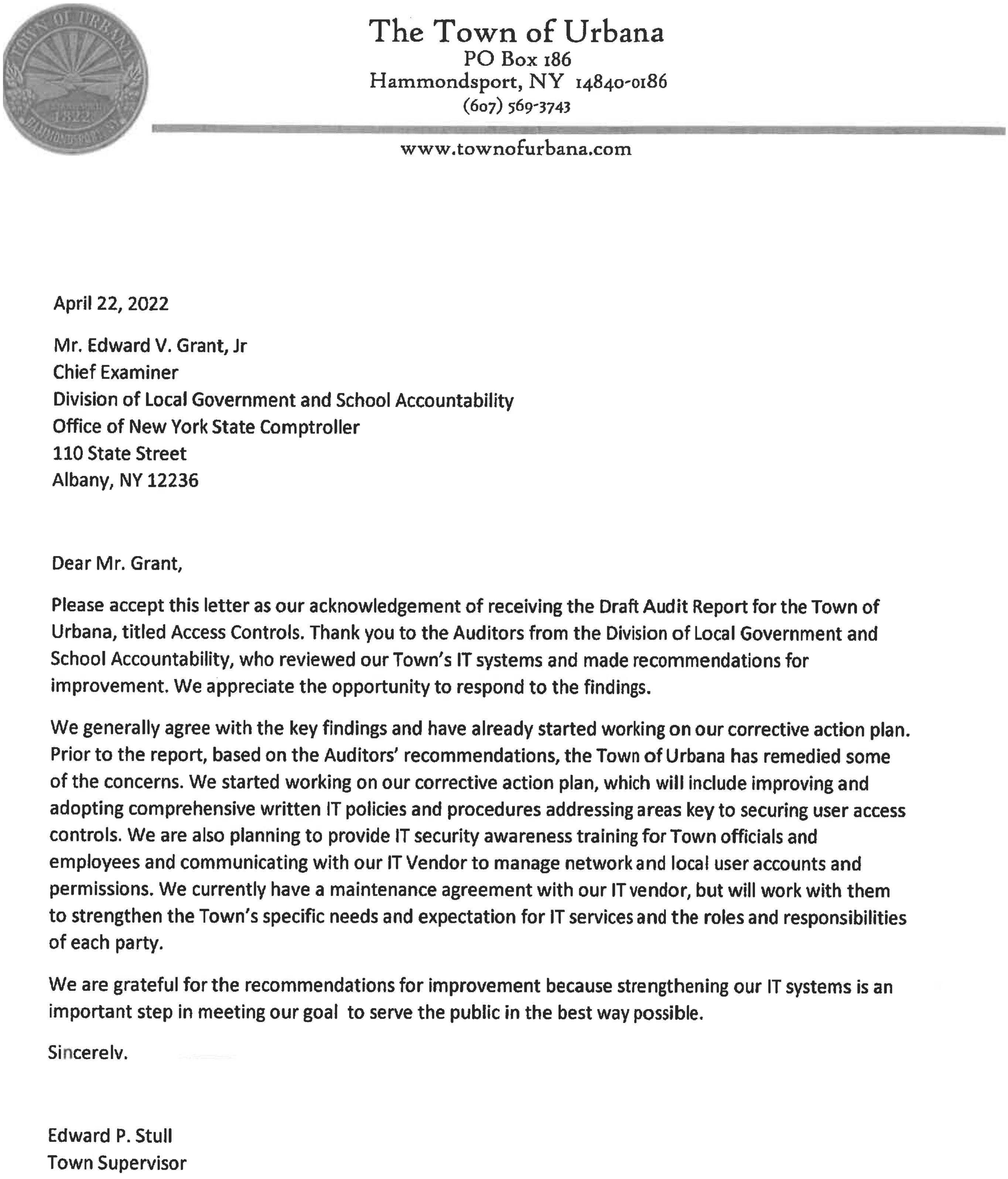
2. Ensure all Town computer users receive comprehensive IT security awareness training.

3. Adopt comprehensive written policies and procedures for managing network and computer user accounts, including adding, disabling and changing user access.
4. Establish a comprehensive IT contingency plan, including data backup procedures.
5. Adopt a written online banking policy that provides users a detailed approval process to verify the accuracy and legitimacy of online banking transactions.
6. Ensure banking agreements reflect current operations and provide for adequate controls over online banking transactions.
7. Establish a detailed, clear and comprehensive SLA with the IT vendor to address the Town's specific needs and expectations and the roles and responsibilities of all parties.

Town officials should:

8. Monitor and enforce compliance with the Town's IT policies.
9. Regularly review and update user accounts for necessity and appropriateness and disable those that are no longer needed.
10. Assess user permissions on a regular basis and ensure that user accounts provide users with the minimum permissions needed to perform their job duties.
11. Monitor the services provided by the IT vendor to ensure expected on-site visits occur and services are provided.

Appendix A: Response From Town Officials



The Town of Urbana
PO Box 186
Hammondsport, NY 14840-0186
(607) 569-3743

www.townofurbana.com

April 22, 2022

Mr. Edward V. Grant, Jr
Chief Examiner
Division of Local Government and School Accountability
Office of New York State Comptroller
110 State Street
Albany, NY 12236

Dear Mr. Grant,

Please accept this letter as our acknowledgement of receiving the Draft Audit Report for the Town of Urbana, titled Access Controls. Thank you to the Auditors from the Division of Local Government and School Accountability, who reviewed our Town's IT systems and made recommendations for improvement. We appreciate the opportunity to respond to the findings.

We generally agree with the key findings and have already started working on our corrective action plan. Prior to the report, based on the Auditors' recommendations, the Town of Urbana has remedied some of the concerns. We started working on our corrective action plan, which will include improving and adopting comprehensive written IT policies and procedures addressing areas key to securing user access controls. We are also planning to provide IT security awareness training for Town officials and employees and communicating with our IT Vendor to manage network and local user accounts and permissions. We currently have a maintenance agreement with our IT vendor, but will work with them to strengthen the Town's specific needs and expectation for IT services and the roles and responsibilities of each party.

We are grateful for the recommendations for improvement because strengthening our IT systems is an important step in meeting our goal to serve the public in the best way possible.

Sincerely,

Edward P. Stull
Town 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 interviewed officials to gain an understanding of IT operations, specifically those related to granting, modifying and revoking user accounts and permissions.
- We obtained and reviewed the Board-adopted AUP.
- We ran a computerized audit script on eight Town computers on August 13, 2021. We then analyzed the results generated by the scripts to obtain information about the computers' local user accounts, including their permissions and security settings, to determine whether they were necessary and appropriate. We also reviewed user accounts to identify inactive and potentially unnecessary accounts and permissions.
- We examined network user account and security settings using a computerized audit script run on August 13, 2021. We reviewed the network user accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts and permissions.
- We followed up with officials to determine whether there were any unneeded local or network user accounts or permissions and any mitigating controls.
- We also inquired of officials about the process for transferring user accounts.
- We obtained and reviewed the Town's agreement with its IT vendor.
- We requested the Town's banking agreements and reviewed those provided to determine any security procedures and authorized personnel.

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

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, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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