REPORT OF EXAMINATION | 2021M-190

Town of Ulysses

Information Technology

APRIL 2022

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

Contents

Report Highlights

Town of Ulysses

Audit Objective

Determine whether Town of Ulysses (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.

- The Board did not adopt adequate written IT policies or a written IT contingency plan.
- Officials did not adequately manage local user accounts.
- The Board did not enter into a written service level agreement with the Town's IT service provider.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive written IT policies, including a written IT contingency plan.
- Regularly review local user accounts and disable those that are unnecessary.
- Enter into a written service level agreement with the Town's IT service provider.

Town officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The Town is located in Tompkins County and is governed by an elected five-member Board including the Town Supervisor. The Board is responsible for overseeing Town operations and finances, including IT operations.

An IT consultant provides IT services for the Town related to monitoring and managing the server, backups, local user accounts, software programs, hardware/software updates and any other IT-related issues as needed.

Quick Facts

On-site Servers and User Computers	14
Employees	26
Local User Accounts Reviewed	46
Payments to the IT Consultant During Audit Period	$7,685

Audit Period

January 1, 2020 – April 30, 2021. We extended our audit period forward through June 17, 2021 to complete our IT testing.

Information Technology

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. We reviewed IT settings for nine on-site computers at the Town – one Town server computer, five Town user computers used by various Town officials and employees, and three user computers used by the Town Justice and court clerk. The Court computers were provided by the New York State Unified Court System's (UCS) Office of Court Administration (OCA),[1] which is responsible for purchasing, distributing, supporting and upgrading the computer equipment for all town and village courts throughout the State.

What Policies and Procedures Should the Board Adopt to Help Secure and Protect IT Systems?

IT policies, such as acceptable use, password security, wireless security, remote access,[2] mobile computing and removable device policies, describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board should establish such policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

A board should consider people, processes and technology that form the town's unique computing environment when determining the content of its IT policies. Further, a 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.

A written IT contingency plan typically includes an analysis of business processes and continuity needs, instructions, specific roles of key individuals and precautions needed to recover data and quickly resume operations in the event of an unplanned disruption. The plan should be tested periodically and updated as appropriate to ensure officials understand their roles and responsibilities during a disruptive event, such as a major natural disaster (e.g., flood, fire) or software or hardware failure caused by a computer virus or human error.

1 OCA is the administrative arm of UCS. The Division of Technology is a unit within OCA that provides technology services for UCS, including town and village courts.

2 Remote access is when a user accesses an IT system from a physical location other than that of the system.

The Board Did Not Adopt Adequate IT Policies or an IT Contingency Plan

IT Policies – The Town's IT policies addressed acceptable use but lacked clear expectations and guidance about the following:

- Password complexity, length and age requirements and the number of failed log-on attempts the system will allow. Without clear expectations and guidance, the risk is increased that users could select short and simple passwords that never expire which would increase the likelihood that an attacker could successfully guess or otherwise determine a targeted password. In addition, if unlimited log-on attempts are allowed, potentially malicious individuals would have more opportunities to guess or crack a password.
- Conditions that wireless devices must satisfy and who (e.g., all employees, contractors, consultants, temporary and other workers) is authorized to connect to the Town's network. The lack of this guidance could lead to unauthorized access to the Town's network.
- Specifying who is authorized to have remote access, the rules and requirements for connecting remotely and the approval process for granting access. This lack of guidance could lead to an increased risk of unauthorized access and compromises to the Town's data.
- Controls over mobile computing and removable devices that contain or access information resources. The lack of this guidance could lead to unauthorized access to information resources.

Officials told us that they believed that the policies covered in the Town's employee handbook sufficiently covered IT issues, and they were not aware of the IT policies that they were missing. A lack of appropriate policies detailing the Board's expectations significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Without properly designed and functioning internal controls, there is a likelihood that significant errors or fraud could occur and remain undetected.

We reviewed the Internet use and web history on a sample of nine out of the Town's 14 on-site computers and, aside from minor discrepancies discussed with Town officials, determined that the usage and web histories were for appropriate and allowable Town purposes.

IT Contingency Plan – The Board did not develop a written IT contingency plan to document processes and inform Town officials how they should respond to unplanned disruptions. Consequently, in the event of a disaster, ransomware attack or other unplanned event, staff have insufficient guidance or plans to follow to recover data and resume essential operations in a timely manner. Officials

stated that they relied on the IT consultant and data backup procedures to protect the Town's data and had not formally documented procedures to respond to potential disruptions. Without a comprehensive written plan, officials and employees are not informed of the expected procedures to follow in the event of an unplanned disruption. As a result, the Town has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees, due to improper or insufficient recovery efforts.

How Should Officials Manage User Accounts?

Town officials are responsible for restricting user access to only those applications, resources and data needed to complete job duties and responsibilities. This helps ensure data and IT assets are protected from unauthorized use and/or modification. Local user accounts enable computers and certain applications to recognize specific users and accounts and provide user accountability by affiliating user accounts with specific users or processes. These accounts are potential entry points for attackers because, if compromised, they could be used to access and view data stored on the computer.

To minimize the risk of unauthorized access, officials should actively manage user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner.

Officials Did Not Adequately Manage Local User Accounts

Officials did not adequately manage local user accounts. This occurred because officials did not inform the IT consultant, who they relied on to manage local user accounts, of necessary changes. As a result, the Town had unneeded and unused local user accounts that had not been disabled and/or monitored.

We judgmentally selected nine out of the 14 on-site Town and Court computers and identified 46 local user accounts.[3] Six local user accounts on Town computers were for former employees. Officials told us that these user accounts were not disabled because they needed access to files saved on the user accounts. However, officials could transfer files from former employees' user accounts prior to disabling the user accounts.

When unnecessary local user accounts are not disabled in a timely manner, there is a greater risk of unauthorized access to personal, private and sensitive information (PPSI) and compromises to IT resources.

Without a comprehensive written plan, officials and employees are not informed of the expected procedures to follow in the event of an unplanned disruption.

3 Refer to Appendix B for further information on our sample selection.

Why Should the Board Have a Written Service Level Agreement with the Town's IT Service Provider?

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

An SLA is a written contract that establishes comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides 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 processes; and pricing, billing and terms of payment.

The SLA should be periodically reviewed, especially when the town's IT environment or needs change significantly.

The Board Did Not Have a Written Service Level Agreement with the Town's IT Service Provider

The Board used the services of an IT consultant who agreed to fix computers, install new hardware and software, make recommendations for purchases, perform updates and backups and maintain the server on an as-needed basis. However, the Board did not have a written SLA with the consultant and only a verbal agreement.

Without a written SLA, the Board and IT service provider do not have stated responsibilities and procedures for how to resolve any failures in IT controls, service disruption or data breach. This can contribute to confusion over who has responsibility for the various aspects of the Town's IT environment, which could put the Town's computer resources and data at greater risk for unauthorized access, misuse or loss.

Without a written SLA, the Board and the IT service provider do not have stated responsibilities and procedures for how to resolve any failures in IT controls, service disruption or data breach.

What Do We Recommend?

The Board should:

1. Adopt comprehensive written IT security policies to address password security, wireless security, remote access and mobile computing and removable devices.

2. Develop and adopt a comprehensive written IT contingency plan.

3. Develop a written SLA with the IT service provider to address the Town's specific needs and expectations for IT services and the roles and responsibilities of the parties.

The Board should designate appropriate personnel to:

4. Periodically assess local user accounts and permissions to ensure unnecessary accounts are disabled as soon as there is no longer a need for them.

Appendix A: Response From Town Officials

TOWN OF ULYSSES
10 Elm Street, Trumansburg, NY 14886
ulysses.ny.us

Town Supervisor (607) 387-5767, Ext 232 supervisor@ulysses.ny.us
Town Clerk (607) 387-5767, Ext 221 clerk@ulysses.ny.us

March 10, 2022

Ann C. Singer, Chief Examiner
Office of the New York State Comptroller
Division of Local Government & School Accountability
Binghamton Regional Office
State Office Building, Room 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear Chief Examiner Singer:

Thank you to the Division of Local Government and School Accountability for reviewing our records in 2021, and we appreciate the opportunity to respond to your findings.

IT/Cyber security is deeply important to the well-being and security of our community, and it touches all parts of our government operations. As a small municipality, we are grateful for the time and consideration given to our IT/Cyber Security issues, and the detailed recommendations about how we can improve our systems to better serve the public. We do not dispute the findings reflected in the report, and have provided our Correction Action Plan (CAP) in this letter of acknowledgement.

Corrective Action Plan

Prior to receiving the report, the Town of Ulysses has already undertaken a number of steps to remedy concerns identified in the report.

We have formed an IT/Cyber Subcommittee and appointed members to oversee our response and make policy and procedural recommendations to the Town Board for implementation.

Our IT service provider has upgraded our Town computer systems and addressed inefficiencies.

During budget development in the fall of 2021, the Town Board determined and created a budgetary line in the 2022 budget to hire an IT Consultant to development a plan to address issues both currently identified and still unknown issues. Additionally, the Town added cyber protection to our insurance coverage.

The Board Should:	Who	What	When
Adopt comprehensive written IT security policies to address password security, wireless security, remote access and mobile computing and removable devices.	Ulysses Town Board, with advice from the Cyber/IT Subcommittee and legal counsel	Comprehensive written IT security policies, which will include specifics regarding password security, wireless security, remote access and mobile computing and removable devices	A preliminary version will be adopted by July 31, 2022. We anticipate modifying and improving the policies after the completion of our IT consultant's review of Town system in 2023.
Develop and adopt a comprehensive written IT contingency plan.	Ulysses Town Board, with advice from the Cyber/IT Subcommittee and legal counsel	A comprehensive written IT contingency plan.	A preliminary version will be adopted by December 31, 2022. We anticipate modifying and improving the policies after the completion of our IT consultant's review of Town system in 2023.
Develop a written SLA with the IT service provider to address the Town's specific needs and expectations for IT services and the roles and responsibilities of the parties.	Ulysses Town Board, with advice from the Cyber/IT Subcommittee and legal counsel	A written SLA with the IT service provider to address the Town's specific needs and expectations for IT services and the roles and responsibilities of the parties.	Contractual language is already in development. Contracts will be issued to service providers by May 31, 2022, with the intention of being fully completed by June 30, 2022.
Periodically assess local user accounts and permissions to ensure unnecessary accounts are disabled as soon as there is no longer a need for them.	Cyber/IT Subcommittee; IT Service Provider	Local user accounts and permissions will be periodically assessed to ensure unnecessary accounts are disabled as soon as there is no longer a need for them.	Completed for Town (excluding Court) computers as of March 10, 2022; will be completed periodically as needed.

Thank you for the opportunity to outline our plan for corrective action concerning the issues identified in your report. We look forward to serving as a model in the future to IT/Cyber best practices, and appreciate the time and attention of your office.

Sincerely,

Katelin Olson, Town Supervisor
Town of Ulysses, NY

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 Board minutes, policies and the Town's employee handbook, and we interviewed Town officials and the IT consultant to obtain an understanding of IT operations and determine the adequacy of IT-related policies and procedures.
- We judgmentally selected nine computers (one Town server computer, five Town user computers and three Court user computers) that were frequently used by Town officials and employees and examined computer settings for 46 local user accounts using specialized audit scripts run on June 9, 2021 and June 17, 2021:
  - We ran a web history computerized audit script on nine computers and then reviewed the Internet use and web history to evaluate whether Internet use was appropriate and if unnecessary exposure of PPSI had occurred.
  - We ran a configurations computerized audit script on nine computers. We then analyzed the results generated by the scripts to obtain information about the computers' user accounts to determine whether local user account and security settings were necessary and appropriate. We reviewed local user accounts to identify unused and potentially unnecessary accounts. We also analyzed local user accounts and security settings applied to those accounts.

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

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

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

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