REPORT OF EXAMINATION | 2020M-127

City of Johnstown

Information Technology

MARCH 2021

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

Contents

Report Highlights

City of Johnstown

Audit Objective

Determine whether City of Johnstown (City) officials safeguarded information technology (IT) resources to ensure personal, private and sensitive information (PPSI) was protected.

Key Findings

City officials did not adequately safeguard IT resources to ensure PPSI was protected. The failure to protect PPSI can have significant consequences on the City, such as reputation damage, lawsuits, a disruption in operations or a security breach. City officials did not:

- Develop adequate IT policies and procedures or provide IT security awareness training.
- Have a complete and accurate IT asset inventory.
- Properly manage user accounts or ensure unneeded administrative and user accounts were disabled.
- Have a written contract or service level agreement (SLA) with the IT service provider to define responsibilities.
- Develop or adopt a disaster recovery plan to minimize the risk of data loss or suffering a serious interruption of services.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop adequate IT policies and procedures.
- Enter into a written contract with the IT provider.
- Develop and adopt a comprehensive written disaster recovery plan.

City officials were given an opportunity to respond to our findings and recommendations within 30 days of the exit conference, but they did not respond.

Background

The City is located in Fulton County. The City is governed by an elected Common Council (Council) composed of a Mayor, a Council member-at-large and four Council members who represent each of the City's wards.

The Council is responsible for general management and control of City operations. The Mayor is the chief executive officer responsible, along with other administrative staff, for day-to-day administration.

The City outsources IT operations to an IT provider. The IT provider is responsible for general IT support and managing the City-wide and Police Department networks. The IT provider reports to the City Treasurer (Treasurer).

Quick Facts	
Network User Accounts	92
Total Paid to the IT Provider During the Audit Period	$92,309

Audit Period

January 1, 2019 – January 15, 2020

Information Technology

City officials and employees use City-owned IT assets (e.g., computers, laptops and tablets) to perform day-to-day operations and access and store information collected by the City. The City uses its computer system to collect and store data received and produced from its operations, which includes PPSI[1] and employee data and relies on its IT system for Internet access, email and maintaining financial records.

If the system is compromised the results can be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls do not guarantee the safety of the computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems can be lost or damaged by inappropriate access and use.

…[C]ity officials should adopt a computer use policy that describes appropriate and inappropriate use of IT resources…

How Should IT Resources Be Safeguarded?

A city's governing body should establish computer policies that take into account people, processes and technology. The governing body should communicate these policies throughout the city's departments, and ensure city officials develop procedures to monitor compliance with the policies.

Specifically, city officials should adopt an acceptable use policy that describes appropriate and inappropriate use of IT resources, consequences of violating the policy, access to PPSI, storage devices and online banking and monitor compliance with that policy.

City officials should maintain records of IT assets (i.e., computers) documenting, at a minimum, what equipment the city has and where it is located. Detailed records make verifying the existence of IT assets easier and demonstrates to employees that management is monitoring purchases and use, deterring theft and misuse. Officials should ensure employees responsible for purchasing IT assets are made aware of the individuals responsible for maintaining IT asset records.

In addition, city officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the city's Internet and IT systems and data, and informs employees of security risks and practices that reduce internal and external threats to IT systems and data. The content of training programs should be directed at the specific audience (e.g., user or system administrator) and include everything related to IT security that attendees need to know to perform their jobs.

1 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.

City officials are responsible for restricting user access to only those resources and data that are necessary for their day-to-day duties to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. Officials should develop comprehensive written procedures for managing system access that include periodic reviews of user access to ensure that network user accounts are disabled or changed when access is no longer needed.[2] When employees leave city employment, officials should ensure that these accounts are disabled in a timely manner.

Similarly, officials should develop written procedures for classifying, accessing, storing and disposing of PPSI. These procedures should define PPSI, explain the city's reasons for collecting PPSI and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities. As part of classifying data, city officials should develop and maintain an inventory of PPSI, identifying where it is stored on the network and who uses it to help determine how to protect it.

Officials Did Not Develop Adequate IT Polices or Procedures

Although the employee manual requires City-owned computers and email accounts to be used for appropriate business purposes only, officials did not develop adequate written IT policies or procedures. We reviewed the IT section of the employee manual and found that it did not include guidance related to access to PPSI, password security, wireless devices, mobile computing and storage devices and online banking or describe the consequences for policy violations.

In addition, while employees were required to sign an acknowledgment form for receipt of the employee manual, our review of seven personnel folders disclosed that only two acknowledgment forms were signed.[3] Further, officials did not provide users with IT security awareness training.

City officials cannot protect the confidentiality, integrity and availability of data and computer systems without developing and implementing adequate IT security policies and procedures to ensure users, or those who manage IT, understand these policies and procedures and their roles and responsibilities related to IT and data security.

2 Network user accounts are used to access computers and other resources on a network.

3 Refer to Appendix B for details on our sampling methodology.

When there are inadequate policies to clearly describe the consequences of policy violations and employees are not properly trained, enforcing any such policies may be difficult and the system, data and PPSI could be at a greater risk for unauthorized access, loss or misuse.

In addition, because City officials did not provide users with IT security awareness training to help ensure they understood IT security measures designed to safeguard online activity, IT assets and data and PPSI were more vulnerable to loss and misuse.

Officials Did Not Maintain a Complete and Accurate IT Asset Inventory

While City officials did not maintain an inventory of IT assets, the IT provider gave us an inventory list that we determined was incomplete. For example, the Fire Department uses tablets for their daily operations that were not on the inventory list.

The Treasurer told us that departments purchase their own IT equipment and do not always inform the IT provider. Without a complete and accurate inventory of IT assets, City officials cannot be assured that these assets are adequately accounted for and information on these assets are protected.

Officials Did Not Adequately Manage Network User Accounts

City officials did not adequately manage network user accounts to safeguard data from potential abuse and loss. Specifically, City officials did not develop procedures for granting, changing and disabling user permissions to the network. In addition, officials did not review network user account permissions to ensure they were appropriate and were unaware certain users were granted unnecessary administrative permissions and other permissions not needed to perform their job duties.

We reviewed all 92 enabled network user accounts and found 27 of these accounts were not needed and should have been disabled. In addition, 11 other accounts had unneeded permissions. Specifically, we found the following:

- 10 accounts (11 percent) were unnecessarily assigned administrative permissions.[4]

4 Having administrative permissions means a user has privileges to perform most, if not all, functions within an operating system on a computer. These privileges can include such tasks as installing software and hardware drivers, changing system settings and installing system updates. They can also create user accounts and change their passwords.

- Five were generic accounts.[5]
  - Four were temporary accounts for software vendors that did not need these permissions.
  - One account was an unused IT provider account that was not needed.
- Five accounts belonged to City officials or employees who did not need administrative permissions to perform their job duties.

- 20 accounts (22 percent) were generic accounts.
  - For 18 of these accounts, City officials were unaware of account use or could not provide sufficient user information and 13 appeared to be unnecessary because they were not used in the last six months.
  - Two accounts provided unnecessary access to certain users.[6]
- 13 accounts (14 percent) belonged to City employees or officials who left City employment between one and six years before our review and were unneeded.
  - Nine accounts were used to access the network after the employee left City employment. The Treasurer and the IT provider were unable to provide us with supporting documentation or explanations for this activity.

Nine [network user] accounts were used to access the network after the employee left City employment.

Because City officials did not regularly review user accounts or have procedures for granting, changing and disabling user permissions, unnecessary accounts went unnoticed. When unneeded network user accounts exist, there is a risk that these accounts could be used as entry points for attackers to access PPSI and compromise IT resources.

In addition, when employees have unnecessary administrative permissions, there is an increased risk that unauthorized changes could occur or PPSI could be used inappropriately and the compromise of an account with administrative permissions could cause greater damage than with a lesser-privileged account because these accounts have full control over the network or user computer.

5 Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if necessary.

6 These accounts were shared by all Fire Department employees for training purposes.

Officials Did Not Adequately Protect PPSI

City officials did not classify or maintain an inventory of PPSI and where it is stored. Additionally, because user permissions were not adequately managed or monitored, users were granted unnecessary access to PPSI that was not needed to perform their job duties.

For example, one secretary had access to PPSI because she worked for the Fire Department and was grouped with other Fire Department employees, all these employees were granted access to PPSI whether they needed access to perform their job duties or not. The secretary did not require access to PPSI to perform her job duties.

We reviewed nine network user accounts on 11 computers to determine whether the account users had needed access to PPSI and complied with the City's employee manual for appropriate Internet use.[7] Eight of these accounts provided users with access to PPSI. One account was a shared network user account accessed by 31 users, only some of these users needed access to PPSI.

We identified instances of personal Internet use on all 11 computers unrelated to City business. This included access to entertainment, leisure, personal shopping and social media websites. Some access to entertainment and leisure websites included access to inappropriate content by one user that violated the City's policy (outlined in the employee manual) for acceptable Internet use.

The IT provider told us they enforced the City's policy by blocking websites that would be considered obscene or X-rated. Although the City has a web filter,[8] it was not used to its full potential because City officials did not provide the IT provider with guidelines to restrict access to certain types of websites.

Without a PPSI inventory, City officials cannot ensure that all PPSI is properly accounted for and protected. Furthermore, Internet browsing increases the likelihood of exposing computer systems to malicious content that could compromise PPSI or the system. The failure to protect PPSI can have significant consequences on the City, such as reputation damage, lawsuits, a disruption in operations or a security breach.

City officials did not classify or maintain an inventory of PPSI and where it is stored.

7 Refer to Appendix B for information on our sampling methodology.

8 A web filter stops users from viewing certain websites by preventing their browsers from loading pages from these websites.

Why Should Officials Have a Written Contract or SLA with the IT Provider?

A written contract between a city and its IT provider provides both parties with a clear understanding of the services expected to be provided and a legal basis for compensation provided for those services. The council should have a formal written contract that specifies the contract period, the services to be provided and provides the basis of compensation for those services.

In addition, to protect the city and avoid potential misunderstandings, officials should have a written SLA between the city and its IT provider that identifies the city's needs and expectations, including those relating to confidentiality and protection of PPSI, and specifies the level of service to be provided by the IT provider.

An SLA differs from a traditional written contract in that it establishes comprehensive, measureable 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 process; pricing, billing and terms of payment.

Officials Did Not Have a Written Contract or SLA with the IT Provider

City officials have relied on an IT provider for IT services, technical assistance and purchase of IT equipment, as needed, for over 10 years without a written contract or SLA. The Council did not negotiate a written contract with its IT service provider and officials did not enter into an SLA with the provider to identify the specific services to be provided or the provider's responsibilities.

The City paid the IT provider $92,309 during our audit period including a $1,250 monthly service fee.[9] However, except for two four-hour on-site visits each month, officials were unable to identify the services included in the monthly fee. As a result of our inquiry, the IT provider gave the Treasurer a written list of services included and not included in this fee.

9 The City paid the IT provider $37,138 for equipment and supplies, $18,829 for software renewals and warranty, $15,000 for monthly services, $9,717 for technical support, $5,355 for software services, $4,018 for hardware installation and $2,252 for backup services.

In addition, officials did not monitor the services provided by the IT provider to ensure the on-site visits occurred and other services were provided, as expected. The IT provider provided assistance with, among other things, hardware and software issues, setting up new desktops and installing applications during visits. However, City officials did not log or otherwise track the on-site visits or services provided to determine whether the expected visits were provided or additional visits occurred that should have been covered by the monthly service fee.

The IT provider's invoices lacked specific detail itemizing the services covered by the monthly service fee, including on-site visits, and the IT provider reported concerns to the Treasurer rather than directly communicating with the Council. The Treasurer only communicated information to the Council when it involved significant or costly changes to the system.

Without a written contract and direct communication with the Council, the roles and responsibilities of each party were not defined and City officials failed to ensure the IT provider fulfilled their obligations. The lack of an agreement can contribute to confusion over who is responsible for the various IT environment aspects, which ultimately puts the City's IT assets and data at a greater risk for unauthorized access, misuse or loss.

To minimize the risk of data loss or suffering a serious interruption of service, city officials should establish a formal written disaster recovery plan.

Why Should the City Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event (such as a fire, computer virus or inadvertent employee action) that compromises the availability or integrity of an IT system and data.

To minimize the risk of data loss or suffering a serious interruption of services, city officials should establish a formal written disaster recovery plan. The disaster recovery plan should address the potential for sudden, unplanned catastrophic events that could compromise the network and availability or integrity of city services, including the IT system and data.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures and periodic backup testing to ensure they will function as intended.[10] Backup data should be stored at a secure offsite location, maintained off-network and encrypted to ensure its integrity. The plan should be periodically tested and updated to ensure key city officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

10 A backup is a copy of electronic information that is maintained for use if there is a loss or damage to the original.

Officials Did Not Have a Disaster Recovery Plan or Adequate Backup Procedures

City officials have not developed and adopted a disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover vital data for City government operations. Officials told us the City's IT provider is responsible for monitoring, storing and restoring the daily and weekly backups, stored both onsite and offsite. However, while the IT provider encrypted the data stored onsite, the offsite data was not encrypted during transmission to the offsite storage location and the IT provider has not tested or restored backups.

Without a formal written plan, responsible parties may not be aware of steps they should take, or how to continue doing their jobs to resume business in the event of disaster. Also, by not testing backups, City officials have no assurance that important data will be available in the event of a loss. As a result, the City has increased risk that it could lose important data and suffer a serious interruption in operations.

What Do We Recommend?

The Council should:

1. Develop and update IT policies to provide guidance related to access of PPSI, password security, wireless devices, mobile computing and storage devices and online banking. Communicate these policies to City officials, employees and the IT provider and routinely (at least once per year) review and update them to reflect changes in technology and the City's computing environment.

2. Enter into a written contract with the IT provider that sufficiently defines the roles and responsibilities of each party, specifies IT service pricing and includes all services to be provided.

3. Develop and adopt a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

City officials should:

4. Ensure that all employees sign a form acknowledging receipt of an updated employee manual, as required.

5. Provide periodic IT security awareness training to all personnel who use IT resources, addressing the City's IT policies, personal Internet browsing, the importance of physical security over IT resources and protection of PPSI.

6. Maintain a complete and accurate IT hardware asset inventory.
7. Develop comprehensive written procedures for granting, changing and disabling network user permissions that include periodically reviewing user access and disabling or changing accounts when access is no longer needed.
8. Develop written procedures for classifying, accessing, storing and disposing of PPSI.
9. Develop and maintain an inventory of PPSI and protect it by granting access based on job duties and monitoring users' Internet browsing.
10. Establish procedures to ensure all backups are encrypted and routinely tested.

Appendix A: 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[11] and obtain valid audit evidence, our audit procedures included the following:

- We interviewed City officials, employees and the IT provider and reviewed the employee manual to obtain an understanding of the City's IT operations and related policies and procedures, determine whether policies and procedures were adequate and whether City personnel received IT security awareness training.
- We used our professional judgment to select five department heads and two individuals with unnecessary access to PPSI and reviewed personnel folders for acknowledgement forms to determine whether employees acknowledged receipt of the employee manual.
- We reviewed the list of services provided by the IT provider to gain an understanding of the services provided.
- We used our professional judgment to select nine network user accounts on 11 computers and the server. We analyzed and assessed these accounts using specialized audit software to determine whether users had appropriate access to PPSI and identify any inappropriate Internet use. We selected City officials, department heads, employees and the account used on one computer accessed by all 31 employees within the Fire Department based on access to PPSI, authority to request changes in user access (add/modify/disable) and to ensure we reviewed at least one account from each department.
- We compared results of our analyses to a current payroll report to identify unnecessary accounts.
- We reviewed all the invoices paid to the IT provider during our audit period to identify the equipment purchased and the services provided.
- 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 City 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 Council 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 Council to make the CAP available for public review in the City Clerk's office.

11 We also issued a separate audit report, *City of Johnstown – Financial Management* (2020M-134).

Appendix B: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

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?title=&body_value=&field_topics_target_id=263206&issued=All

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/sites/default/files/local-government/documents/pdf/2020-05/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?title=&body_value=&field_topics_target_id=263211&issued=All

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

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

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