DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-166

Poughkeepsie City School District

Information Technology

JULY 2020

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

Contents

Report Highlights

Poughkeepsie City School District

Audit Objective

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

Key Findings

- The District did not adequately control and secure its personal, private and sensitive information (PPSI).
- District employees were not provided with IT security awareness training.
- The District did not have service level agreements (SLAs) with its IT service providers.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Inventory, classify and develop effective controls over PPSI.
- Ensure all necessary personnel receive up-to-date IT security awareness training.
- Ensure that all IT services are provided based on a formal service level agreement.

District officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Poughkeepsie City School District is located in the City of Poughkeepsie (City) in Dutchess County (County). The District is governed by a Board of Education (Board), which has five elected members.

The Superintendent is appointed by the Board and is the District's chief executive officer. He is responsible for the day-to-day management of the District, under the Board's direction.

An Assistant Superintendent is responsible for supervising the District's IT Department. This department works with the District's IT service providers to help ensure the District's IT needs are addressed.

Quick Facts	
School Buildings	9
Employees	600
Students	4,300
Network Accounts[a]	683

[a] These included employee and generic accounts, which are used by network services and applications to run properly. Students used shared network accounts to access the District's network.

Audit Period

July 1, 2017 – February 19, 2019. We extended our audit period forward through May 30, 2019 to complete our IT testing.

Information Technology

The District relied on its IT system for Internet access, email and for maintaining financial and personnel records. The District annually contracted with two IT service providers: the Dutchess County Board of Cooperative Educational Services (DC BOCES), which maintained the District's student information system, and the Mid-Hudson Regional Information Center (MHRIC), which provided data warehousing to the District.

The District faces several risks if its IT system is not secure from malicious attack. For example, personal, private and sensitive information (PPSI)[1] of students and faculty could be stolen, grades and transcripts could be altered, unauthorized banking transactions could be executed and/or ransomware attacks could occur. Given the prevalence of these threats, it is imperative for the District to secure its IT system. It is important to note that the procedures used to protect the system – such as adopting and enforcing appropriate policies, providing IT security awareness training and establishing control over contracts with service providers – are generally low-cost steps that can significantly enhance the District's IT system security.

How Does an Acceptable Use Policy Secure and Protect the District's IT Systems?

A school district should have an acceptable computer use policy (AUP) that defines the procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy. In addition, officials should require employees to sign acknowledgement forms to indicate they read the District's AUP and are aware of what is expected of them and to acknowledge they will be held accountable for compliance with the policies and procedures outlined in the AUP.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by monitoring Internet usage. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, acceptable use policies or standard security practices.

Monitoring for AUP compliance involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Automated mechanisms may be used to perform this process and can help security professionals routinely assess

[1] PPSI is any information to which unauthorized access, disclosure, modification or destruction – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access.

Officials should periodically review IT policies, update them as needed and stipulate who is responsible for monitoring policy compliance. The District's policy manual stated that employees should use District-owned computers and email accounts "for appropriate purposes only."

Officials Did Not Monitor for AUP Compliance

District officials did not monitor employee Internet use or implement procedures to monitor for compliance with the District's stated AUP. In addition, officials could not provide any evidence that network users had read, were aware of and acknowledged they would be held accountable to the AUP.

We reviewed the web browsing history of 20 computers assigned to 19 employees[2] and found that all 19 employees accessed websites that appeared personal in nature. We also conducted an analysis of shared network folders[3] and found folders that contained music and video files that included popular movies and TV shows, which were not being used for District purposes.

District officials were unaware of this inappropriate computer use because they did not routinely monitor employee Internet use or the content of network folders. In addition, because officials did not require employees to sign or otherwise acknowledge receipt of the AUP, network users might not have been aware of the AUP, which increases the risk of exposing the District's IT systems and data to loss or misuse.

Internet browsing increases the likelihood of computer systems being exposed to malicious software that may compromise PPSI. As a result, the District's computer system and any PPSI it contains have a higher risk of exposure to damage and PPSI breach, loss or misuse.

Why Should the District Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, District officials should establish a formal written disaster recovery plan (plan). This is particularly important given the current and growing threat of ransomware attack. The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computers virus or inadvertent employee action) that could compromise the network and the availability or integrity of the financial systems and any student, faculty or other PPSI contained therein.

[2] One employee was assigned two computers. We reviewed both computers assigned to this individual. Refer to Appendix B for further information on our sample selection.

[3] These are folders on the network that can be accessed by several individuals.

Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary precautions needed to take to maintain or quickly resume operations. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

Officials Did Not Have a Disaster Recovery Plan

District officials did not develop a comprehensive written plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster, officials have no guidelines or guidance to minimize or prevent the loss of equipment and data. While officials acknowledged they did not have a plan, they told us they intended to create one during the process of updating District policies and procedures.

Without a formal plan, officials cannot guarantee that in the event of a disaster they would be able to restore critical IT systems, applications or data in a timely manner. Depending on the severity of an incident, officials may need to expend significant time and financial resources to resume District operations. Furthermore, essential employees may not be aware of their roles, which could complicate the District's ability to recover from an incident. As a result, the District has an increased risk that it could lose important data and suffer serious interruption in operations.

Why Should Officials Provide IT Security Awareness Training to Employees?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district 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 employees and students. The training should center on emerging trends such as information theft, social engineering attacks[4] 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 everything that attendees need to perform their jobs.

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

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

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

In addition, the Board and officials should establish a policy and written procedures that require employees to be trained in IT security awareness issues and in proper usage of the IT infrastructure, software and data. While IT policies will not guarantee the safety of the District's systems, without formal policies and procedures that explicitly convey the appropriate use of the District's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Officials Did Not Provide IT Security Awareness Training

District officials did not provide employees with IT security awareness training to help ensure they understand IT security measures designed to safeguard data from potential abuse or loss and their role in protecting District assets. We interviewed 20 employees[5] to determine whether they received or were offered IT security awareness training by the District and found that none had received or were offered this type of training from the District.

Due to high personnel turnover, officials did not know why IT security awareness training was not being provided to employees. The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District 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, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data, PPSI and IT assets could be at greater risk for unauthorized access, misuse or loss.

Why Should the District Have a Service Level Agreement (SLA) With its IT Service Providers?

To protect the District and avoid potential misunderstandings, officials should have a written SLA between the District and its IT service provider that identifies the District's needs and expectations and specifies the level of service to be provided.

An SLA is different 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

[5] Refer to Appendix B for further information on our sample selection.

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; and pricing, billing and terms of payment.

The SLA should be reviewed by knowledgeable IT staff, legal counsel, or both, and be periodically reviewed, especially if the IT environment or needs change significantly.

District Officials Did Not Have SLAs With the District's IT Service Providers

The Board did not negotiate formal agreements or SLAs with DC BOCES and MHRIC to identify the vendors' responsibilities and specific services to be provided because it was unaware of the benefits of having such agreements. Instead, District officials chose IT products and services from each vendor by selecting certain items from a vendor checklist. However, the checklist did not provide detailed explanations of the services.

Therefore, officials had no way of knowing whether any services overlapped between the two providers and could not choose how the services were provided. Also, they could not have compared whether they were receiving the best value for similar goods and services offered by other IT vendors.

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

Why Should the District Maintain Accurate and Up-To-Date Inventory Records?

Computer hardware management is of particular importance to larger entities such as school districts that have many different users who perform a variety of functions. Maintaining complete and comprehensive inventory records is crucial in safeguarding IT assets from loss or theft.

Officials should maintain detailed, up-to-date inventory records for all computer equipment to safeguard IT assets. Information maintained for each piece of computer equipment should include a description of the item, including make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; physical location of the asset; and relevant purchase information; such as acquisition date and asset value. Each item should be affixed with an identification tag, and the tag's number should be included in the item's inventory record.

Officials should verify the accuracy of inventory records through periodic physical inventory counts. Also, equipment should be periodically examined to establish condition and to verify accurate location information in the inventory records. Maintaining complete and up-to-date IT inventory records also helps the board develop and implement an effective technology replacement plan.

Officials Did Not Maintain Adequate Inventory Records

Prior to our audit, the District did not have inventory records for its IT assets. During our audit, District officials contracted with a vendor to record and tag all District equipment. When this was completed, we reviewed the new inventory list and found that serial numbers, locations of equipment and names of individuals assigned to the equipment were missing for about half of the equipment on the list.

During our review of 20 computers,[6] we searched for their serial numbers in the new inventory list and found only three. The serial numbers of the remaining 17 computers (85 percent) were not included in the new inventory list.

Without an accurate inventory of computers and technology equipment, officials cannot be assured that assets are accounted for and protected from loss, theft and misuse. Furthermore, in the event of a loss, officials would be unable to provide their insurance carrier with an accurate list of assets or determine the items that needed to be replaced.

Why Are Online Banking Agreements Important?

Online banking allows users to access their bank accounts to review current account balances and account information and transfer money between bank accounts and to external accounts. Because funds transferred electronically typically involve significant amounts of money, district officials must control the processing of its electronic transfers to help prevent unauthorized transfers from occurring.

New York State General Municipal Law (GML)[7] allows school districts to disburse or transfer funds by electronic transfers, provided that the governing board enters into a written agreement with the district's bank. GML requires that this agreement describe the manner in which electronic transfers will be accomplished and

[6] Ibid.

[7] GML, Article 2, Section 5-A

identify the names and numbers of bank accounts from which transfers may be made and the individuals authorized to request transfers. Also, GML requires school districts to implement a security procedure that includes verifying that payment orders are for the initiating district and reviewing payment orders to detect errors in transmission or content.

School districts should check with their banks about enabling alerts and other security measures that may be available, such as blocking wire transfers to foreign countries, sending email notifications of electronic transfers and requiring verification of transactions over certain amounts, possibly through a call to a designated individual.

Officials Did Not Have an Adequate Banking Agreement

District officials maintained seven bank accounts with one bank for online banking transactions, which included electronic deposits, interaccount transfers and electronic withdrawals. We found that the District was in violation of GML because it did not have an online banking agreement with the bank with which it conducted business. In addition, officials did not establish security controls such as blocking transfers to foreign countries.

Officials told us they were unaware that GML required the District to have an online banking agreement with its bank. Without an adequate online banking agreement that includes established security controls, officials are exposing the District's bank accounts to unnecessary risk. Furthermore, without established policies officials cannot ensure that authorized employees will understand their roles when performing online bank transactions.

How Can Officials Protect Online Banking Transactions?

The Board should adopt an online banking policy that describes authorized online banking activities, specifies which employees are authorized to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of online transactions and describes what type of computing devices should be used to perform online banking transactions.

To the extent possible, authorized users should access bank accounts from one computer dedicated for online banking from a wired network to minimize exposure to malicious software, because other computers may not have the same security protections as a dedicated computer.

With a dedicated computer, officials could limit the software installed on that computer to programs needed for online banking activities and restrict use of the computer for activities unrelated to online banking, including checking email and browsing the Internet. Furthermore, online banking should not be conducted from personal devices because officials cannot monitor these devices and ensure they are secure.

Officials Did Not Adequately Safeguard Online Banking Transactions

All District online banking users were required to enter a username, password and unique passcode that were generated each time they logged into the District's online banking application. Although these are effective controls, the District did not have a policy that lists employees who are authorized to process transactions and that requires a detailed approval process to verify the accuracy and legitimacy of transactions before they are processed.

In addition, employees did not use a dedicated separate computer for online banking activities, and users were not prohibited from accessing District bank accounts online with personal devices. When employees use multiple computers for online banking and other unrelated activities, it increases the possible opportunities for the District's online bank accounts to be exposed to attackers through additional software installed on the multiple computers and increased number of email messages opened and websites visited by employees.

In addition, when employees use non-District devices, such as personal laptops or smartphones, to perform District online banking activities, the District does not have any guarantee that those devices and their online connections are adequately secured and protected from malware and other unauthorized activities.

The District did not have an online banking policy because officials did not consider the importance of implementing one. Without sufficient policies, procedures, and security controls, District officials cannot ensure that funds are adequately safeguarded during online bank transactions.

What Do We Recommend?

The Board should:

1. Consider amending the AUP to indicate that employees should not store, share or download personal files onto computers and network folders.

2. Adopt an online banking policy that describes authorized online banking activities, specifies which employees are authorized to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of online transactions and describes what type of computing devices should be used to perform online banking transactions.

District officials should:

3. Ensure that sufficient written banking agreements that address online banking with each bank are in accordance with GML, and that those who perform online banking transactions are familiar with its content.

4. Monitor employees’ computer use and implement procedures to monitor for compliance with the District’s AUP.

5. Ensure that all network users sign an acknowledgement that they read and acknowledged they would be held accountable to the AUP.

6. Periodically review shared network folders to ensure their contents are appropriate.

7. Develop a comprehensive, written disaster recovery plan that provides specific guidelines for the protection of IT assets and data against loss or destruction.

8. Ensure employees receive formal IT security awareness training on an ongoing basis that reflects current risks identified by the IT community.

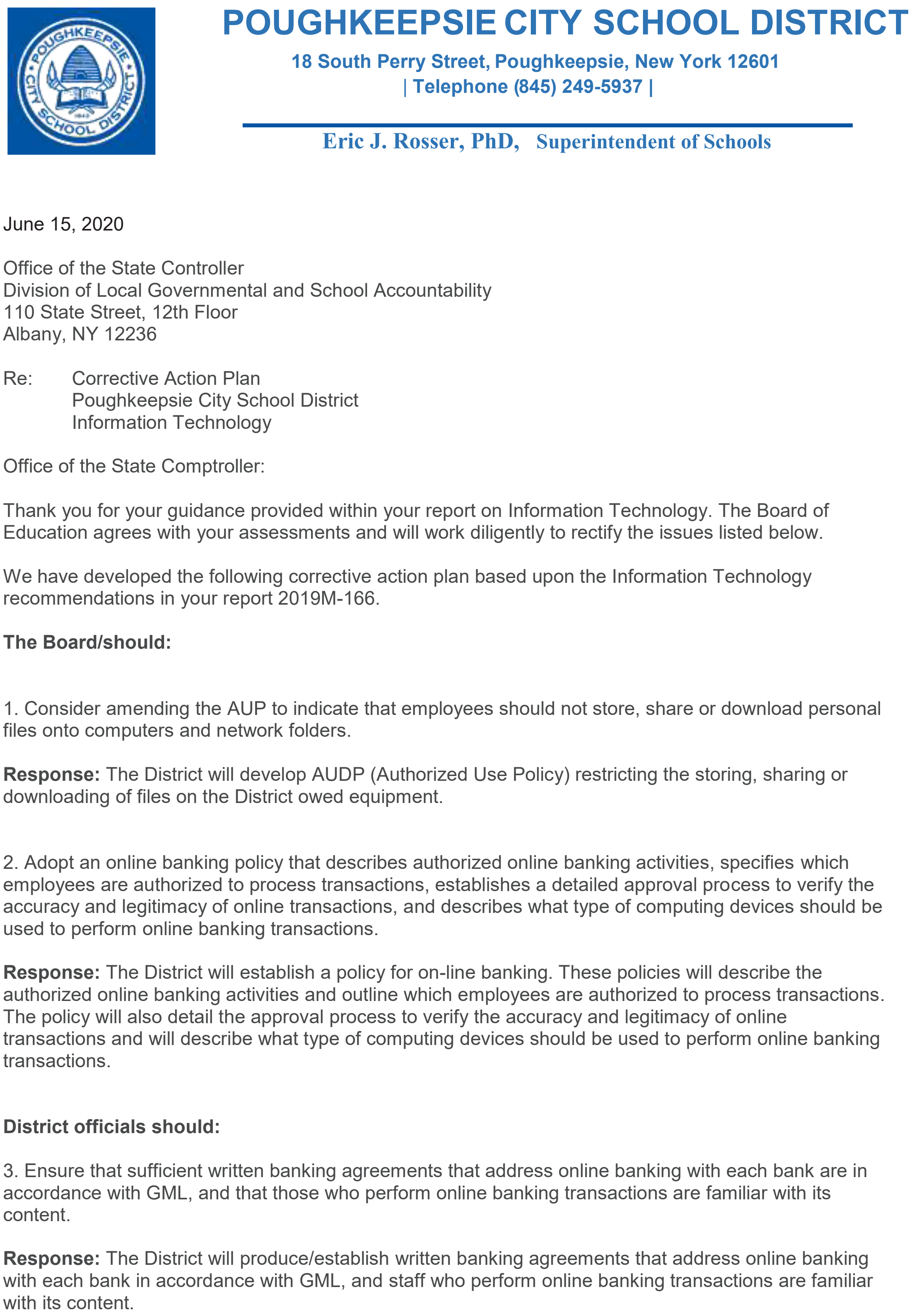
9. Develop an SLA with DC BOCES and MHRIC to address the District’s specific needs and expectations for IT services and the roles and responsibilities of all parties.

10. Develop a comprehensive, up-to-date inventory list that includes serial numbers, locations of equipment and names of individuals assigned to the equipment.

11. Establish a sufficient written online banking agreement, in accordance with GML, with each bank the District uses for online banking transactions, and ensure employees who perform online banking transactions are familiar with its content.

12. Dedicate a separate computer for online banking activities and limit all online banking to that computer.

Appendix A: Response From District Officials



POUGHKEEPSIE CITY SCHOOL DISTRICT

18 South Perry Street, Poughkeepsie, New York 12601
| Telephone (845) 249-5937 |

Eric J. Rosser, PhD, Superintendent of Schools

June 15, 2020

Office of the State Controller
Division of Local Governmental and School Accountability
110 State Street, 12th Floor
Albany, NY 12236

Re: Corrective Action Plan
Poughkeepsie City School District
Information Technology

Office of the State Comptroller:

Thank you for your guidance provided within your report on Information Technology. The Board of Education agrees with your assessments and will work diligently to rectify the issues listed below.

We have developed the following corrective action plan based upon the Information Technology recommendations in your report 2019M-166.

The Board/should:

1. Consider amending the AUP to indicate that employees should not store, share or download personal files onto computers and network folders.

Response: The District will develop AUDP (Authorized Use Policy) restricting the storing, sharing or downloading of files on the District owed equipment.

2. Adopt an online banking policy that describes authorized online banking activities, specifies which employees are authorized to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of online transactions, and describes what type of computing devices should be used to perform online banking transactions.

Response: The District will establish a policy for on-line banking. These policies will describe the authorized online banking activities and outline which employees are authorized to process transactions. The policy will also detail the approval process to verify the accuracy and legitimacy of online transactions and will describe what type of computing devices should be used to perform online banking transactions.

District officials should:

3. Ensure that sufficient written banking agreements that address online banking with each bank are in accordance with GML, and that those who perform online banking transactions are familiar with its content.

Response: The District will produce/establish written banking agreements that address online banking with each bank in accordance with GML, and staff who perform online banking transactions are familiar with its content.

4. Monitor employees' computer use and implement procedures to monitor for compliance with the District's AUP.

Response: The District believes it has strong filtering tools in place but has not actively monitored employees' usage. We will immediately increase monitoring of users' web access.

5. Ensure that all network users sign an acknowledgment that they read and acknowledged they would be held accountable to the AUP.

Response: The District agrees with this recommendation and will have users sign a new/updated AUP on an annual basis.

6. Periodically review shared network folders to ensure their contents are appropriate.

Response: Shared folders will be reviewed on a quarterly basis for content and logs will be maintained.

7. Develop a comprehensive, written disaster recovery plan that provides specific guidelines for the protection of IT assets and data against loss destruction.

Response: A Disaster Recovery Plan (DRP) will be developed district wide along with encouraging staff to make use of the cloud. Recent developments have only increased the urgency to have a DRP immediately.

8. Ensure employees receive formal IT security awareness training on an ongoing basis that reflects current risks identified by the IT community.

Response: The District will institute formal IT security awareness training on an ongoing basis that reflects current risks identified by the IT community. Attendance will be required, logged, and maintained to assure all staff have proper security training.

9. Develop an SLA with DC BOCES and MHRIC to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties.

Response: SLA's have been agreed upon with MHRIC. We are working with Dutchess BOCES to develop SLA's with them.

10. Develop a comprehensive, up-to-date inventory list that includes serial numbers, locations of equipment and names of individuals assigned to the equipment.

Response: The District have an inventory of all IT equipment. We currently use a system offered by Follett, which seems to be working well. We will make sure this IT equipment is part of our overall fixed asset counts and will be tracked for location purposes.

11. Establish a sufficient written online banking agreement, in accordance with GM, with each bank. District uses for online banking transactions and ensure employees who perform online banking transactions are familiar with its content.

Response: The District will produce/establish written banking agreements that address online banking with each bank in accordance with GML, and staff who perform online banking transactions are familiar with its content.
12. Dedicate a separate computer for online banking activities and limit all online banking to that computer.

Response: The District will look into using 1 computer specifically for banking purposes. Unfortunately, there will be times when remote transactions occur. For remote transactions, the Director of Finance will be notified of its occurrence which is expected to be infrequent.

Dr. Eric Jay Rosser
Superintendent of Schools

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 for resolutions concerning IT matters and reviewed District policies to determine the number and scope of policies that were officially adopted.
- We interviewed officials and employees to obtain an understanding of District IT operations.
- We reviewed District records for any IT-related policies and procedures.
- We interviewed District employees to determine whether there were any safeguards were in place to protect sensitive data and financial assets.
- We reviewed 19 employees' Internet use on the 20 computers[8] assigned to them to evaluate whether their Internet use was in compliance with the District's acceptable use guidelines. We used our professional judgment to select seven employees based on job titles that indicated duties likely to involve accessing student, staff and financial PPSI.[9] While we were working with the seven employees who we selected using our professional judgment, there were several other employees working in the same locations. We randomly chose the remaining 12 employees in our sample from these locations. We did not select employees who were actively teaching students to avoid disturbing classroom activities. We also interviewed these 19 employees and an additional employee chosen randomly to determine whether they had received formal IT security awareness training.
- We ran a computerized audit script on the District's domain controller.[10] We then analyzed the report, generated by the script, for inactive users. We also compared it to the employee master list to determine whether any network users were no longer employed by the District.
- We ran a shared folders audit script on the District's domain controller. We analyzed the report, generated by the script, to identify any folders that could potentially have contained files that indicated misuse of District computers. We then determined who had access to those folders and verified the contents of the folders with District officials.

[8] One employee in our sample was assigned two computers.

[9] These users had access to applications or systems containing PPSI, including online banking, payroll, human resources, student information and financial systems.

[10] The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

- We reviewed any existing agreements between the District and its IT vendors to determine the scope of services, reporting requirements, performance indicators and security procedures to be provided.
- We asked officials whether the District had a disaster recovery plan.
- We asked officials whether the District had any written agreements with its banks. We also asked officials whether the District had an online banking policy.
- We reviewed user access and permissions for the online banking application and determined whether there was a proper segregation of duties and whether granted user permissions were necessary for the employees to perform their assigned duties.

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 Board 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 must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-1(3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the fiscal year. 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 District clerk’s office.

Appendix C: 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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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