REPORT OF EXAMINATION | 2022M-61

Adirondack Central School District

Information Technology

AUGUST 2022

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

Contents

Report Highlights

Adirondack Central School District

Audit Objective

Determine whether Adirondack Central School District (District) officials implemented adequate information technology (IT) controls over the District's network to help safeguard personal, private, and sensitive information (PPSI).

Key Findings

District officials did not establish adequate IT controls to help safeguard PPSI. In addition to sensitive IT control weaknesses communicated confidentially, we found:

- An IT service provider was paid $526,500 but officials did not have a written service level agreement (SLA) to clearly identify the provider's responsibilities and specific services to be provided.
- Officials did not implement adequate IT controls to manage network user accounts. Of the 343 network accounts reviewed, 64 accounts were not needed.
- The Board did not adopt an IT contingency plan. Therefore, a cyber incident could result in the loss of data and serious operational interruption.
- The District had three policies that detail the proper usage of IT assets. The polices are not consistent and seven of 13 computers were used for personal use.

Key Recommendations

- Establish adequate polices, plans and agreements needed to protect the Districts IT network and data.

District officials generally agreed with our recommendations and indicated they are initiating corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

Background

The District serves the Towns of Ohio, Russia, and Webb in Herkimer County; the Towns of Lewis, Leyden, Lyonsdale, and West Turin in Lewis County; and the Towns of Annsville, Ava, Boonville, Forestport, Lee, Remsen, Steuben, and Western in Oneida County.

The District is governed by a seven-member Board of Education (Board) that is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is the chief executive officer and responsible for District administration. The Director of Technology, Curriculum, and Instruction (Director) is responsible for managing the District's IT operations.

Quick Facts

2020-21 Fiscal Year	
Amount Spent on Third-Party IT Services	$526,500
Enabled Accounts	
Students	887
Non-Student	343
Total	1,230
Reviewed During Audit	343
Not Needed	64

Audit Period

July 1, 2020 – November 9, 2021

Information Technology

IT systems and data on the District's network are valuable resources. The District relies on its IT systems for maintaining financial, personnel and student records, email and Internet access. Some of the records and files maintained by the District's IT systems contain PPSI. 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.

If the IT systems and data are compromised, the results could range from inconvenient to catastrophic and could require extensive efforts and resources to evaluate, repair and rebuild. While effective IT controls will not guarantee the safety of an IT system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

The District contracts with Madison-Oneida Board of Cooperative Educational Services (BOCES) for IT-related services provided by the Mohawk Regional Information Center (MORIC). These services included but were not limited to: firewall and intrusion detection; data support services; financial and student information system support; security awareness training; and Internet access and filtering.

The Director should have sufficient experience with the IT environment, have knowledge of the cybersecurity risks and threats currently facing school districts and how to mitigate these risks. The Director, along with two full-time computer specialists, are responsible for overseeing the District's general computer system operation.

School district officials must ensure they have qualified IT personnel to implement IT controls, manage and help secure the school district's IT environment and safeguard PPSI.

Why Should a District Have an SLA With Its IT Service Provider?

School district officials must ensure they have qualified IT personnel to implement IT controls, manage and help secure the school district's IT environment and safeguard PPSI. This can be accomplished by using school district employees, an IT service provider or both. To help protect a school district's network and avoid potential misunderstandings, officials should have a written SLA with the school district's IT service provider that clearly identifies the school district'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 so that there is a mutual understanding of the nature and required level of services to be provided. It should provide detailed explanations of the services to be performed by identifying the parties to the agreement 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. Additionally, the SLA should be monitored to ensure the services paid for are provided.

The District Did Not Have an SLA with BOCES

The Superintendent and Director could not provide us with a formal agreement or SLA with BOCES to identify responsibilities and specific services to be provided by MORIC. District and MORIC officials provided us with various statement of assurances and cooperative service agreement (COSER) descriptions for IT services, however, the assurances and COSERs did not state detailed information for services to be provided to the District. They also did not explain District and MORIC responsibilities, or include comprehensive, measurable performance targets. Instead, District officials had a list of IT products and services that were being provided by MORIC through BOCES for the 2020-21 fiscal year, totaling approximately $526,500. Without an SLA, it is difficult for officials to monitor whether the District received the appropriate level of services for the costs incurred.

District officials did not negotiate a comprehensive written SLA with BOCES to identify responsibilities and specific services to be provided by MORIC because they were unaware of the benefits of having such an agreement. Without an adequate SLA, the District and MORIC 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, including PPSI, at greater risk for unauthorized access, misuse or loss.

How Should District Officials Manage Network User Accounts and Permissions?

Network user accounts are an IT control which enable networks, connected computers, and certain applications to recognize specific users and processes, allow network administrators to grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users and processes. Network user accounts are potential entry points for attackers because, if compromised, they could be used to access, and view data, including PPSI, stored on the network.

School district officials are responsible for restricting network user account access to only those network resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data, including PPSI, and IT assets are safeguarded and protected from unauthorized use and/or modification. A school district should have written procedures for granting, changing and removing user access and permissions to the network.

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

Service and shared network user accounts are not linked to an individual. For example, service user accounts are accounts created for the sole purpose of running a particular network or system service or application (e.g., backup systems). Shared user accounts are accounts with a username and password that are shared among two or more users and are often used to provide access to guests and other temporary or intermittent users. Officials should routinely evaluate service and shared network user accounts and disable those that are not related to a current school district or system need.

Generally, an administrative account has permissions to monitor and control a network, connected computers, and certain applications with the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, any program that a user with administrative permissions runs could inherently run with the same permissions. For example, if malicious software (malware) installed itself on a computer, it may run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of network or computer compromise and/or data loss. Therefore, it is especially important for officials to regularly review administrative accounts and promptly disable them when they are no longer needed.

Cybersecurity risks should be treated like any other hazard a school district may encounter along the way. School district officials should identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the superintendent, the board, and the IT department.

Officials Did Not Properly Manage Network User Accounts and Permissions

District officials did not implement adequate IT controls to manage network user accounts and permissions on the District's network or user computers to help

safeguard PPSI. The District does not have written procedures for granting, changing, and removing individual rights to the network. Additionally, the IT Department does not regularly review network user accounts to ensure the accounts are needed and the permissions are necessary. The computer specialist told us that when an employee is terminated or otherwise leaves District employment, the District Clerk will inform the computer specialist, authorizing the IT Department to disable the employee's network user account. Likewise, when an employee needs their access rights modified, the District Clerk also informs the computer specialist of the changes.

Unneeded Network User Accounts – We reviewed all 343 non-student network user accounts for necessity and appropriateness. With the assistance of one of the District's computer specialists and MORIC Security Leader, we determined that 64 of the 343 network user accounts (19 percent) were unneeded. Forty-eight of the 64 unneeded user accounts belonged to former employees or third-party consultants who no longer worked for or provided services to the District. The remaining 16 unneeded accounts were service and shared user accounts. Of the 64 unneeded user accounts, 14 have never been used to log into the network and another 41 user accounts had not logged into the network in the last six months. After our review, the computer specialist and MORIC Security Leader stated all 64 accounts were either disabled or deleted.

…[W]e determined that 64 of the 343 network user accounts (19 percent) were unneeded.

Unnecessary Administrative Permissions – Of the 11 network user accounts with network administrative permissions, three user accounts were no longer needed and one user account did not need administrative permissions. Three user accounts belonged to MORIC employees who no longer needed the accounts, and one was a service account. The computer specialist told us that while the service account was needed, it did not need administrative privileges, therefore, the administrative rights were revoked.

We also reviewed the necessity and appropriateness of another 12 network user accounts that had local administrative permissions on 12 computers. The local administrative permissions were unnecessary for four of the 12 user accounts. One of the four user accounts belonged to a former employee, and the remaining three belonged to current District employees who did not need the elevated permissions.

Because there were no procedures in place for IT Department staff to regularly review network user accounts and permissions, the unneeded network user accounts and unnecessary administrative permissions were not identified until our audit.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. The compromise of a network user account with administrative

permissions could cause greater damage than the compromise of a lesser-privileged account because administrative accounts have full control over the network, computer or application. Also, when a District has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access.

Why Should the District Adopt an IT Contingency Plan to Help Safeguard PPSI and IT Systems?

An IT contingency plan is an IT control representing a school district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations and data, including PPSI, 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, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the school district's operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident and could significantly reduce the resulting impact.

The goal of an IT contingency plan is to enable the recovery of an IT system and/ or electronic data, including PPSI, as quickly and effectively as possible following an unplanned disruption. Because IT often supports key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive written IT contingency plan should focus on strategies for sustaining a school district'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. Written policies and procedures are also critical components and help ensure that information is routinely backed up and available in the event of a disruption.

Typically, an IT contingency plan should address the following key components:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Identifying and prioritizing critical business processes and services,
- Communication protocols with outside parties,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,

- Detailed backup procedures, and
- Details concerning how the plan will be periodically tested.

The District Did Not Adopt an IT Contingency Plan

The Board did not adopt a comprehensive written IT contingency plan to describe the procedures and technical measures officials would take to respond to potential disruptions affecting IT. Consequently, in the event of a disruption or attack (e.g., ransomware), District officials and employees have insufficient written guidance to restore or resume essential operations in a timely manner and help minimize damage and recovery costs.

Officials were unable to provide a reasonable explanation for not having a comprehensive written IT contingency plan in place. Without a formal plan, there is an increased risk that the District could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees, and the loss or potential compromise of student and employee PPSI.

How Does an Acceptable Use Policy (AUP) Help Safeguard PPSI?

A school district should have a written AUP that defines the procedures for computer, Internet and email use to help safeguard PPSI. The AUP should describe appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP. Monitoring compliance with the AUP should involve regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity, or availability. School district officials can reduce the risks of PPSI exposure or compromise by monitoring Internet use and by configuring web filtering software to block access to unacceptable websites and, to the extent possible, limit access to sites that comply with the school district's AUP.

District Computers Were Used for Personal Activities

The District had three separate AUPs, which were located in the District's policy manual, technology plan and the employee handbook. All three AUPs address the appropriate and inappropriate use of IT resources to varying degrees, along with consequences for inappropriate use, such as loss of access. However, they use different language and, therefore, could be confusing to those expected to adhere to them. For example, the AUP in the employee handbook states the District's network "shall be used for only education purposes consistent with the district's

mission and goals," whereas the AUP in the technology plan specifies users "will not use the computer system for personal use." The AUP in the policy manual is similar to the technology plan, but it does not include the same computer user rules, which make it clear the computer systems should not be used for personal use. The Superintendent, Director and Business Administrator told us they were not aware that there are three different versions of the AUP.

Employees are provided a copy of the AUP located in the employee handbook at the beginning of their employment with the District, and at the beginning of each school year. New employees are required to sign a document indicating that they will abide by the Acceptable Use Agreement and that employees should not expect privacy when using the system. Annually, employees are also required to sign a document indicating that they have read and familiarized themselves with the contents of the District's handbook; the signed document is maintained at the District office.

Although the District uses web filtering software to block access to some prohibited websites, certain categories of websites that could be accessed for non-District purposes, such as shopping, entertainment and travel, were not blocked because they were occasionally used for business or educational purposes. Despite this limitation, the Director did not ensure logs of Internet use were periodically reviewed for appropriateness, and as a result, did not implement adequate IT controls to help safeguard PPSI.

We reviewed the Internet browsing history on 10 employees' computers (total of 13 computers). We selected these employees because their job duties required them to regularly access or have access to PPSI. We identified five employees (seven computers) who accessed websites not related to District operations. Two of these employees had significant personal use of the Internet across three computers. Employees' personal use included accessing websites related to entertainment, non-District travel, personal shopping, personal email, and personal online banking.

Employees' personal use included accessing websites related to entertainment, non-District travel, personal shopping, personal email, and personal online banking.

Additionally, District officials did not ensure all employees signed an AUP form at the beginning of their employment and at the beginning of each school year. For example, the District Clerk provided us documentation showing that eight of 10 employees sampled signed an AUP form. The District Clerk could not provide signed AUPs for the remaining two employees, who both accessed websites not related to District operations. After our inquiry, the District Clerk obtained signed AUPs from these two employees.

When employees access websites for non-business or non-instructional purposes through the network, in violation of the District's AUPs, productivity may be reduced and there is an increased risk that IT assets and users' information or PPSI that users have access to could be compromised through malicious

software infections. For example, if a user were to inadvertently download a malicious software program from the Internet, or click on a malicious attachment in a personal email account, it could infect the user's computer and potentially other computers connected to the District's network. This could allow individuals to steal information or gain unauthorized access to sensitive information, such as social security numbers and bank account information.

What Do We Recommend?

The Board and District officials should:

1. Develop a written SLA with BOCES to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties. Ensure that the agreement includes measurable performance targets and the related costs.

2. Develop and adopt a written IT contingency plan that provides adequate guidance on how the District plans to recover its critical IT operations in the event of an unexpected incident. Distribute the plan to all responsible parties and ensure that it is periodically tested and updated as needed.

3. Review the different AUPs and develop and adopt a uniform AUP that clearly describes appropriate and inappropriate use of IT resources and, establish procedures to monitor employee compliance with the AUP.

The Director should:

4. Develop written procedures for granting, changing and removing network user access and permissions.

5. Evaluate all existing network user accounts, disable any deemed unneeded and ensure effective procedures are in place to periodically review all network user accounts and administrative permissions for necessity and appropriateness.

6. Monitor computer Internet use to ensure employees comply with the AUP.

The Director and District officials should:

7. Ensure all officials and employees who use District IT resources sign and return the required AUP forms.

Appendix A: Response From District Officials

Adirondack Central School District
110 Ford Street, Boonville, New York 13309
Tel: 315-942-9200 Fax: 315-942-5522
www.adirondackcsd.org

July 15, 2022

RE: Comptroller Audit Response Letter (Instructional Technology - Adirondack)

To Whom It May Concern:

Adirondack Central School District had an Instructional Technology audit performed. The audit was conducted in the latter part of 2021 through the spring of 2022, and the time period that was analyzed covered July 1, 2020 to November 9, 2021 (a little over a year). The district was provided with the draft public report June 15, 2022.

Overall, the public report has 4 key findings/recommendations:
1-to enhance/improve the Service Level Agreements with greater clarity between the Mohawk Regional Information Center and the District, for the technology the MORIC supports/provides to the District,
2-improve our onboarding and offboarding of new staff and exiting staff to ensure technology accounts/rights are monitored and disabled as appropriate,
3-to improve our IT Contingency Plan and to practice table top exercises to ensure appropriate stakeholders are knowledgeable about the plan in the event of a technology disaster/disruption, and
4-to review policies for acceptable use of district technology to ensure consistency and to assure there's district monitoring/enforcement of the policy.

Overall, the District understands these 4 key areas, is in general agreement, and is in the process of addressing these 4 areas. The Mohawk Regional Information Center, one of 12 regional information centers across the state, is a resource to 49 school districts in Central New York. They will work with and guide Adirondack on improving #1 and #3 mentioned above. We do have Co-Ser Criteria Guidelines Systems for the technology we contract with the MORIC for, but we will work to improve them to the SLA specifications the audit report recommends. In addition, Adirondack has an IT Contingency Plan, using the template provided by the MORIC, but we will work to update it, elaborate on it, and improve it to the recommendations contained in the audit report. Communication and work has already begun between the District and the MORIC. Concerning item #2, all technology accounts have been taken care of that were not needed. In addition, moving forward, the district is in the process of updating our onboarding/offboarding process for all employees, along with scheduling periodic reviews of various technology accounts as a back-up. Finally, item #4 has already been resolved, as the Board approved an updated AUP in the spring of 2022, and all forms match this language. All new staff are required to sign the AUP before they are issued accounts, and annually all staff sign off on the staff handbook, which includes the AUP. The District intends to periodically review 10 staff accounts to monitor compliance.

See Note 1 Page 11

The Adirondack Board of Education will be approving the formal Corrective Action Plan at the August 9, 2022 meeting.
Sincerely,

Kristy W. McGrath

Appendix B: OSC Comment on the District's Response

Note 1

The District did not have a written IT contingency plan. The Cybersecurity Incident Response Plan noted was not finalized or distributed and does not address many key components that would be included in an IT contingency plan.

Appendix C: 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 District officials, MORIC employees, and reviewed the District's IT policies and procedures to gain an understanding of the District's IT controls. We determined whether the District had an SLA agreement with BOCES. We gained an understanding of internal controls related to granting, modifying and disabling network user accounts and permissions. We also determined whether the District had an adequate IT contingency plan and if internal controls were sufficient over the AUP.
- Using our professional judgment, we selected a sample of 13 user computers assigned to 10 District employees. We selected user computers belonging to employees whose job duties required them to regularly access or have access to PPSI. We ran computerized audit scripts on 12 of the computers between August 4, 2021 and August 30, 2021. Because the audit scripts could not run on one of the computers, we took manual screenshots of Internet browsing for a sample week and reviewed the local user permissions on this computer. We then analyzed the results generated by the scripts and the manual screenshots to evaluate whether the Internet browsing on the users' computers was following the District's AUP. We also analyzed the results to determine whether network user accounts with local administrative permissions were necessary and appropriate.
- We ran a computerized audit script on the District's domain controller, on August 4, 2021, to gather network user account information and related security settings. We then analyzed the results generated by the script to obtain information about the District's 343 non-student network user accounts, including their permission and security settings, to determine whether they were necessary and appropriate. We compared the 343 non-student network user accounts to the active employee list to identify user accounts for former employees and other accounts that may be unneeded. We then followed up with District and MORIC staff to assess whether the accounts were needed, and whether administrative permissions were needed for certain 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 District 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-a (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 next 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. The CAP should be posted on the District's website for public review.

Appendix D: 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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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