REPORT OF EXAMINATION | 2021M-137

Morristown Central School District

Information Technology

DECEMBER 2021

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

Contents

Report Highlights

Morristown Central School District

Audit Objective

Determine whether Morristown Central School District (District) officials adequately managed network user accounts and developed an information technology (IT) contingency plan.

Key Findings

District officials did not adequately manage network user accounts or develop an IT contingency plan that details how District officials would respond to IT disruptions. Officials did not:

- Develop written procedures for granting, changing and revoking user access to the overall network.
- Perform periodic reviews of network user accounts to determine whether they were appropriate or needed.

In addition, sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop written procedures for network user access.
- Evaluate and periodically review all network user accounts and disable those that are unneeded.
- Develop a comprehensive written IT contingency plan for the District.

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

Background

The District serves the Towns of DePeyster, Hammond, Macomb, Morristown and Oswegatchie in St. Lawrence County.

The District is governed by a seven-member Board of Education (Board) responsible for the management and control of financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and responsible for District administration.

The District contracts with the St. Lawrence-Lewis Board of Cooperative Educational Services (BOCES) to provide IT services including Internet access, email, network and financial application support and management of the District's network.

A BOCES IT Coordinator (Coordinator) is responsible for managing the District's network server. A BOCES technician is responsible for overseeing the District's network user accounts.

Quick Facts

Total Network User Accounts	
Students	370
Non-Students	109
Unneeded	26

Audit Period

July 1, 2019 – April 2, 2021

Information Technology

A school district relies on its IT assets for Internet access, email, and maintaining financial, student and personnel records, much of which contain personal, private and sensitive information (PPSI).[1] Network user accounts provide users with access to resources on a network and are managed centrally by a server and/or domain controller. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. A domain controller is the main server in the domain (network) that controls or manages all computers within the domain.

A school district should have written procedures for granting, changing and revoking user access and permissions to the network.

Why Should Officials Manage Network User Accounts?

Network user accounts should be actively managed to minimize the risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers and, if compromised, they could be used to access and view PPSI on the network. A school district should have written procedures for granting, changing and revoking user access and permissions to the network. In addition, to minimize the risk of unauthorized access, officials should regularly review enabled network user accounts to ensure they are still needed. When unneeded network user accounts exist, the school district has an increased risk that sensitive information could be intentionally or unintentionally changed and/or compromised by unauthorized individuals. As such, officials should disable unnecessary accounts as soon as there is no longer a need for them.

…[T]he District did not have written procedures for creating, modifying or disabling user accounts on the network and did not adequately manage all network user accounts.

Officials Did Not Adequately Manage All Network User Accounts

The District Principal (Principal), Superintendent and various department supervisors are responsible for monitoring network user accounts and notifying the technician when to create and disable District network user accounts. Officials told us they have informal procedures for user account management, including annual reviews of network accounts that have not been used within 90 days. However, we found these procedures were not always performed or effective.

In addition, the District did not have written procedures for creating, modifying or disabling user accounts on the network and did not adequately manage all network user accounts. We reviewed all 479 network user accounts (370 student accounts, 84 employee accounts, 16 generic and shared accounts and nine contractor accounts assigned to BOCES staff) to determine whether any were unneeded.[2]

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 (students), third parties or other individuals or entities.

2 Refer to Appendix B for information on our testing methodology.

Unneeded Employee Accounts – When new employees are hired or if an employee user account modification is needed, the Superintendent or Principal typically sends an email notification to the technician to add or modify user accounts. In addition, the technician disables user accounts after District officials submit a help desk ticket or provide a verbal notification.

During our review of all 84 employee accounts, we found three enabled network user accounts assigned to former substitute employees that left the District in December 2015, April 2020 and February 2021. The Coordinator told us the network user account for the employee who left in February 2021 was slated for deactivation as part of the annual review of network accounts in the Summer of 2021. In addition, the Principal told us the lack of the network user's account deactivation for the employee who left in April 2020 was an oversight. However, they were not aware of why the network user account for the employee who left in 2015 was not disabled.

Unneeded Student Accounts – When a student is enrolled, the guidance counselor creates a student account in the student information system, which issues an automatic request to the technician to create a corresponding network account. Both accounts are disabled by the guidance counselor and technician using a similar process.

During our review of all 370 student accounts, we found 20 enabled network user accounts assigned to former students who graduated in June 2020. The student information system generated an automatic email informing the technician and District officials of the students who graduated and no longer needed accounts. However, the District did not ensure the unneeded accounts were disabled. The Principal told us lack of follow up was a District oversight.

Unneeded Contractor Account – During our review of the nine enabled network user accounts assigned to BOCES staff, we found one network user account that should have been disabled in 2016 when it was no longer needed. The Coordinator told us that not disabling this account was an oversight error because the disabling of an account typically occurs when there is a change in staff, but there was no change in staff in this instance, and therefore he was not reminded to disable the unneeded user account.

Unneeded Generic and Shared Accounts – During our review of the 16 generic and shared network user accounts, we found two accounts that have not been used in over two years. One account belonged to the Board and the other to a group of substitute employees. The Coordinator told us the Board initially used the shared account to project information on a screen during Board meetings, however the account is no longer used or needed. Further, all employees including substitutes have individual network user accounts and, as such, the

shared account for substitute employees is no longer needed and should be removed from the network.

Because the District's network had unneeded enabled network user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources.

Why Should a District Have a Written IT Contingency Plan?

IT contingency planning involves analyzing business processes in the event of a disruption and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. As part of the contingency planning process and to minimize the risk of data loss or suffering a serious interruption of services, officials should establish a written IT contingency plan that includes guidance on disaster recovery.

The IT contingency plan should address the potential for sudden, unplanned events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the IT system and data. This is particularly important given the current and growing threat of ransomware attacks. In addition, the IT contingency plan should be periodically tested and updated to ensure key officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

The District Did Not Have a Written IT Contingency Plan

The Board did not develop a comprehensive written IT contingency plan to describe the measures District officials would take to respond to potential disruptions and disasters affecting the District's IT environment. While BOCES has a written IT contingency (business continuity) plan that includes recovery methods of hardware, applications, data and connectivity in the event of a disaster for its contracted school districts, the District did not adopt its own IT contingency plan that addresses technical needs and situations unique to the District.

District officials told us they were unaware they needed to develop their own IT contingency plan since BOCES manages their network. While the District may adopt a plan that incorporates the BOCES IT contingency plan, it is important for the District to adopt its own IT contingency plan that addresses the District's own unique IT operations to help ensure services can continue in the event of a disaster.

Without a comprehensive 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 or process student grades and State aid claims.

What Do We Recommend?

District officials should:

1. Develop written procedures for granting, changing and revoking user access to the overall network.
2. Evaluate all existing network accounts, disable any deemed unneeded and ensure effective procedures are in place to periodically review all network user accounts for necessity.
3. Develop and adopt a comprehensive written IT contingency plan for the District and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Appendix A: Response From District Officials

MORRISTOWN CENTRAL SCHOOL
P.O. Box 217, 408 Gouverneur Street
Morristown, New York 13664
Phone: 315-375-8814
Fax: 315-375-8604
Website: www.greenrockets.org

Response Letter and Corrective Action Plan

Attention: Rebecca Wilcox, Chief Examiner
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Unit Name: Morristown Central School District
Audit Report Title: Information Technology
Audit Report Number: 2021M-137

November 12, 2021

Response to Findings:
This District has reviewed the draft audit report, and we are in agreement with the recommendations. The only findings the District would provide a response to is the unneeded student account review. During the July/August period of 2020, the District had a switch in BOCES Technicians. The outgoing technician had a list of 20 graduates to end accounts for; however, when the new technician took over, this was not communicated by the outgoing technician. A procedure was set up to end the 20 June graduates accounts; however, it was not fulfilled during the employee transition. This was rectified immediately upon recognition of the error.

Corrective Action Plan:
For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed. For recommendations where corrective action has not been taken or proposed, we have included the following explanations.

Audit Recommendation 1:
Develop written procedures for granting, changing, and revoking user access to the overall network.

Implementation Plan of Action(s):
Policy #5674 states the District will:
f) Periodically grant, change, and terminate user access rights to the overall networked computer system and to specific software applications and ensure that users are given access based on, and necessary for, their job duties.

The District will revise the policy to read, "the District will yearly grant, change, and terminate user access rights ...." The District will also add a section to our new employee packet and our exiting employee packet to include a date when access was given and when revoked. Student accounts are generated and ended based upon our student management system notification of a new student and/or an exiting student. The BOCES technician receives these emails and completes a help desk ticket when accounts are added and/or ended.

Implementation Date:
December 21, 2021 BOE meeting.

Person Responsible for Implementation:
Staci Vaughn is responsible for BOE policy change. Staci Vaughn and David Doe are responsible for yearly review of users in order to direct technicians to grant, change, or terminate access rights.

Audit Recommendation 2:
Evaluate all existing network accounts, disable any deemed unneeded and ensure effective procedures are in place to periodically review all network user accounts for necessity.

Implementation Plan of Action(s):
All accounts have been reviewed as of 11/01/2021, and the District has disabled any unneeded accounts.

Policy #5674 states the District will:
f) Periodically grant, change, and terminate user access rights to the overall networked computer system and to specific software applications and ensure that users are given access based on, and necessary for, their job duties.

The District will revise the policy to read, "the District will yearly grant, change, and terminate user access rights ...." The District will also add a section to our new employee packet and our exiting employee packet to include a date when access was given and when revoked. Student accounts are generated and ended based upon our student management system notification of a new student and/or an exiting student. The BOCES technician receives these emails and completes a help desk ticket when accounts are added and/or ended.

Implementation Date:
Completed as of 11/01/2021. Policy will be updated at the December 21, 2021 BOE meeting.

Person Responsible for Implementation:
Staci Vaughn is responsible for BOE policy change. Staci Vaughn and David Doe are responsible for yearly review of users in order to direct technicians to grant, change or terminate access rights.

Audit Recommendation 3:
Develop and adopt a comprehensive written IT contingency plan for the District and ensure it is distributed to all responsible parties, periodically tested, and updated as needed.

Implementation Plan of Action(s):
The District has assembled a team responsible for drafting the plan and has identified and prioritized critical business processes and services. The District will develop and distribute the plan to all responsible parties, train as needed, test, and review the plan periodically.

Implementation Date:
The district has drafted the IT contingency plan and will have a final plan developed by January 1, 2022.

Person Responsible for Implementation:
Staci Vaughn and David Doe are responsible for writing and periodically reviewing and testing the comprehensive written IT contingency plan.

Signed:

Staci A. Vaughn
Superintendent

11/12/2021
Date

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, we performed the following audit procedures:

- We interviewed District officials and reviewed the District's IT policies and procedures to gain an understanding of the IT environment, specifically those related to granting, modifying and disabling network user accounts and permissions and to determine whether the District had an IT contingency plan.
- We examined all network user account and security settings on the District's domain controller using a computerized audit script. We analyzed the reports generated to review the network user accounts and compare them to current employee lists to identify inactive and possibly unneeded network user accounts. We also verified network user accounts assigned to BOCES staff were needed and appropriate. We identified any generic accounts that could also be shared accounts. We discussed with District officials the necessity of the network user accounts we reviewed.
- We reviewed user access groups and judgmentally selected one network user account per distinct job title, for a total of 24 network users, to determine whether the users' job titles were compatible with the assigned user access group. We also reviewed all users with administrative permissions to determine whether permissions were appropriate.
- We ran a computerized audit script on the District's domain controller to determine whether the operating system and anti-virus software programs were up-to-date and supported by vendors.

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 GAGAS, generally accepted government auditing standards. 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 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 C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

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