New York State Comptroller
THOMAS P. DiNAPOLI

Chittenango Central School District

Information Technology

2023M-155 | March 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Chittenango Central School District

Audit Objective

Determine whether the Chittenango Central School District (District) officials adequately managed nonstudent network and local user account access and developed an Information Technology (IT) contingency plan.

Key Findings

District officials did not adequately manage nonstudent network and local user account access or develop an IT contingency plan. As a result, the District's IT system and its personal, private and sensitive information (PPSI) may be accessible to unauthorized users. Officials also have less assurance that, in the event of a disruption or disaster such as a ransomware attack, employees and other responsible parties would be able to react quickly and effectively to help resume, restore, repair and/or rebuild critical IT systems or data in a timely manner.

In addition to sensitive IT control weaknesses we confidentially communicated to officials, we determined:

- Eighty-nine (15 percent) of the District's nonstudent network user accounts were no longer needed and should have been disabled.
- Eleven of 21 local user accounts (52 percent) reviewed on 12 District computers were no longer needed.

Key Recommendations

- Disable unneeded nonstudent network and local user accounts as soon as they are no longer needed and periodically review user accounts for necessity.
- Develop and adopt a written IT contingency plan.

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

Audit Period

July 1, 2021 – August 9, 2023

Background

The District serves the Towns of Cazenovia, Lenox, Lincoln and Sullivan in Madison County, and the Towns of Cicero and Manlius in Onondaga County.

The District is governed by an elected nine-member Board of Education (Board), responsible for managing and controlling financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Director of Technology (Director) is responsible for managing the District's IT network, including managing user account access to the network and computers.

Quick Facts	
Total Number of Employees	556
Nonstudent Accounts Reviewed	
Network User Accounts	578
Local User Accounts	21
Total	**599**

Information Technology

A school district (district) relies on its network and other IT assets for maintaining financial, student and personnel records, and Internet access and email, much of which contain PPSI. PPSI is any information to which unauthorized access, disclosure, modification or destruction – or disruption of access of use – could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

Computer and network resources can be accessed using local and network user accounts. A local user account is stored on a server or user computer and grants access to resources on that server or user computer, whereas a network user account grants access to resources on any server, user computer or other IT asset on the network to which that account has access. Both local and network user accounts, if improperly managed, can pose a security risk to the information and overall operation of a computer and network.

Because no computer system can be expected to always operate perfectly, unplanned service disruptions are inevitable. Proactively anticipating and planning for such disruptions will help prepare district personnel for the actions they must take in the event of a disruption that could significantly reduce the resulting impact and serve as a resource that district officials can consult in the event of a disruption or disaster.

How Should District Officials Manage Nonstudent Network and Local User Accounts and Permissions?

District officials should adequately manage all network and local user accounts, including nonstudent network user accounts (e.g., staff, shared and service accounts,[1] third-party vendors), to minimize the risk of unauthorized network and local computer access. Adequate network and local user account management means network access and permissions are only granted to individuals that need access and their permissions are limited to what is needed to perform their job responsibilities and includes user account creation, use and dormancy, and regularly monitoring them to ensure they are appropriate and authorized. User accounts that are no longer needed should be disabled immediately.

District officials should have written procedures for granting, changing and disabling user account access to the network and local computers. These procedures should establish who has the authority to grant or change user account access and require district officials to periodically review enabled user accounts to ensure they are appropriate and authorized.

District officials should have written procedures for granting, changing and disabling user account access to the network and local computers.

1 Service accounts are not linked to individual users and may be needed for certain network services or applications to run properly. Shared accounts are accounts that are used by more than one user for the purpose of logging into a computer system and accessing network resources. For example, service accounts can be created and used for automated backups, while shared accounts may be used for testing processes, training purposes or for shared email accounts, such as a service helpdesk account.

Generally, administrative accounts have oversight and control of the network and/or local computers, with the ability to add new users and change users' passwords and permissions. Users with network and/or local administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. Therefore, district officials should limit users with administrative permissions and regularly monitor all user account access to ensure it is appropriate and authorized.

District Officials Did Not Adequately Manage Nonstudent Network and Local User Accounts and Permissions

District officials did not adequately manage nonstudent network and local user accounts and permissions on the network and user computers. The District had 2,541 enabled network user accounts on the network as of April 11, 2023. With the assistance of the Assistant Superintendent for Business (Assistant Superintendent) and Director, we reviewed all 578 nonstudent network user accounts and their enabled permissions, along with local user accounts and enabled permissions on 12 user computers.

Unneeded Network User Accounts – We identified 89 enabled network user accounts, four of which had administrative permissions, that were no longer needed and should have been disabled (Figure 1). Eighty (90 percent) of the unneeded enabled network user accounts had either never been accessed (logged into) or had not been accessed in over six months. In addition, we determined that nine user accounts had been accessed after the date the account was last needed.

Figure 1: Unneeded Network User Accounts

Network User Account Category	Number of Unneeded Network User Accounts	Number of Unneeded Network User Accounts Disabled
Shared and Service Accounts	39	38
Former District Personnel[a]	31	30
Third-Party Providers[b]	17	15
Duplicate User Accounts	2	2
Total	**89**	**85**

a – Former employees, substitutes, student teachers and a guest speaker.
b – Student information system support staff, Pre-K coordinators and Central New York Regional Information Center (CNYRIC) staff.

We met with the Director and Assistant Superintendent to review and obtain explanations as to why the nine user accounts had been logged into after the date that account access was last needed. We determined that two network user

accounts assigned to former District employees were being used by two current District employees to retrieve information in the former employees' email and files. However, the Director should have collected all necessary information from the email and files after the employees left the District and disabled the user account. When current employees can log into user accounts that are not assigned to them, there is a risk that the user account could be used for inappropriate purposes.

Additionally, three network user accounts were logged into by IT department personnel to sync the network user accounts to the student data server. The Director and Assistant Superintendent, however, could not explain why the remaining four network user accounts were logged into after the date that account access was last needed. These four user accounts were assigned to a former District employee and three non-District employees (two CNYRIC support staff and a guest speaker).

The Director indicated that he disabled all 89 unneeded network user accounts after we informed him of our audit results of our tests; however, we confirmed that 85 of the 89 network user accounts had been disabled and four unneeded accounts still remained enabled as of August 9, 2023. The Director could not provide a reasonable explanation for why the four user accounts were not disabled.

Network User Accounts with Unnecessary Local Administrative Permissions – We reviewed the necessity and appropriateness of 11 network user accounts that had local administrative permissions on five of the 12 user computers. The local administrative permissions were unnecessary for six of the 11 user accounts (55 percent). Four of the 11 network user accounts were no longer needed and had unnecessary administrative permissions on the network (discussed above). The additional two network user accounts included a service account that did not need administrative access for its functionality and an account belonging to a current employee who did not need administrative permissions to perform their job duties.

District officials added or deleted user account access and rights on the network based on a new employee or exiting employee checklist and from an approved substitute list. Additionally, the Director added and removed user account access rights and permissions for student information system support staff based on lists provided by CNYRIC in a shared file with the District that showed when support staff should be added or disabled. However, the Director was not always notified by CNYRIC when the list was updated, so network user accounts used by CNYRIC staff were not always disabled in a timely manner. Although the Director was not always notified by CNYRIC when the list was updated, he should have periodically confirmed he had the most recent list indicating which network user accounts were still needed. Also, there was no clear process for adding, removing or modifying user account access and permissions for other third-party users and student teachers.

While IT staff use the various checklists and documents to initiate user access changes to the network, the Assistant Superintendent and Director told us there were no written procedures to document and formalize the process for adding, removing or modifying network user account access rights and permissions. Furthermore, the Director did not perform an annual review of all enabled accounts to identify accounts that needed to be disabled.

Unneeded network user accounts and network user accounts with unnecessary administrative permissions are additional entry points into a network and, if accessed by attackers, could be used to inappropriately access and view PPSI accessible by those accounts and potentially compromise IT resources. 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 Local User Accounts – Based on our discussion with the Director and our review of the 21 enabled local user accounts on the 12 user computers, we identified 11 local user accounts (52 percent) that were no longer necessary. These 11 unneeded local user accounts also had administrative permissions to the local computer.

The Director told us that IT staff are the only individuals with access to the local user accounts on the computers. However, we identified two local user accounts that did not belong to IT staff. One of the user accounts belonged to a former employee and the other user account belonged to a current employee. The Director did not periodically review local user accounts and permissions, and was unaware of these deficiencies until we brought them to their attention.

When users have unneeded accounts and administrative permissions to computers, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

> Unneeded network user accounts and network user accounts with unnecessary administrative permissions are additional entry points into a network…[and] could be used to inappropriately access and view PPSI. …

Why Should the Board and District Officials Develop and Adopt an IT Contingency Plan?

The board and district officials should develop and adopt a written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. An IT contingency plan is a district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT disruption or disaster. The plan should address the potential for sudden, unplanned disruptions (e.g., system failure caused by inadvertent employee action, power outage, ransomware or other type of malware infection, or a natural disaster such as a flood or fire) that could compromise the network and the availability or integrity of the district's IT system and data.

An IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to recover data and quickly resume operations in the event of an unplanned disruption. Testing and updating IT contingency plans are particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks. The plan should be periodically tested, updated as needed and distributed to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements such as statutory changes.

The Board and District Officials Did Not Develop and Adopt an IT Contingency Plan

The Board and District officials did not develop and adopt an IT contingency plan to describe how officials should respond to potential unplanned IT disruptions and disasters affecting the District's operations that depend on its IT environment. The Director told us that District officials never considered the need for an IT contingency plan in the past.

Without an IT contingency plan, officials have less assurance that, in the event of a disruption or disaster such as a ransomware attack, employees and other responsible parties would be able to react quickly and effectively to help resume, restore, repair and/or rebuild critical IT systems or data in a timely manner. Depending on the severity of an incident, officials may need to spend significant time and financial resources to resume District operations. Furthermore, responsible parties may not be aware of their roles, complicating 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 a serious interruption to operations that depend on its computerized environment, such as not being able to process checks to pay vendors or employees or process student grades.

Without an IT contingency plan, officials have less assurance that, in the event of a disruption or disaster…[they] would be able to react quickly and effectively to help resume, restore, repair and/or rebuild critical IT systems or data in a timely manner.

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

The Director should:

2. Ensure written procedures for granting, verifying, changing and disabling network and local user accounts are established and followed.
3. Disable the unneeded nonstudent network and local user accounts identified in this report and ensure future user accounts are disabled as soon as they are no longer needed.

4. Establish and implement a system to periodically review all existing network user accounts and administrative permissions to determine whether they are needed, and properly disable those that are deemed unneeded.

Appendix A: Response From District Officials

CHITTENANGO CENTRAL SCHOOLS
Michael R. Eiffe, Superintendent
1732 Fyler Road, Chittenango, NY 13037
Telephone: 315-687-2840—Fax: 315-687-2841

ASSISTANT SUPERINTENDENT FOR INSTRUCTION – JASON P. CLARK
315-687-2854
FAX: 315-687-2851

ASSISTANT SUPERINTENDENT FOR BUSINESS – SCOTT MAHARDY
315-687-2846-FAX: 315-687-2845

DIRECTOR OF SPECIAL EDUCATION/PPS – BENJAMIN NEW
315-687-2844
FAX: 315-687-2851

CHITTENANGO HIGH SCHOOL – NICHOLAS FERSCH, PRINCIPAL
JAY ALTOBELLO, ASSOC. PRINCIPAL
315-687-2900
FAX: 315-687-2924

DIRECTOR OF PHYSICAL EDUCATION, HEALTH AND ATHLETICS/DEAN OF STUDENTS – DAVID GRYCZKA
315-687-2905
FAX: 315-687-2924

CHITTENANGO MIDDLE SCHOOL – ARNOLD MEROLA, JR., PRINCIPAL
BRENDON WILLEY, ASSOC. PRINCIPAL
315-687-2800
FAX: 315-687-2801

BOLIVAR ROAD ELEMENTARY – KARA MAY, PRINCIPAL
AMY SUMNER, ASSOC. PRINCIPAL
315-687-2880
FAX: 315-687-2881

BRIDGEPORT ELEMENTARY – MELISSA STANEK, PRINCIPAL
315-687-2280
FAX: 315-687-2281

TRANSPORTATION SUPERVISOR – CONNIE THORP
315-687-2870
FAX: 315-687-5823

FOOD SERVICES DIRECTOR – MATTHEW MORKEL
315-687-2847
FAX: 315-687-2845

DIRECTOR OF FACILITIES – JEFFREY MARTIN
315-687-2860
FAX: 315-687-2861

February 26, 2024

State of New York
Office of the State Comptroller
110 State Street
Albany, NY 12236

Subject: Response to New York State Comptroller's Report of Examination (Report 2023M-155)

Dear Ms. Rebecca Wilcox,

I am writing to formally address the New York State Comptroller's Report of Examination for the Chittenango Central School District (Report 2023M-155). I greatly appreciate the dedicated effort invested by your staff in evaluating our technology procedures, protocols, and best practices covering the period of July 1, 2021 to August 9, 2023. The professionalism and knowledge demonstrated by your staff during the audit were welcomed and appreciated. Additionally, I value the report's comments, suggestions, and recommendations. Moving forward, I will carefully consider all of them.

This response will center on the two (2) recommendations outlined in the report, particularly those discussed in our exit interview held on February 2, 2024. This response to the recommendations will serve as the cornerstone for developing our corrective action plan (CAP).

Comptroller recommendation number one:
Disable unneeded nonstudent network and local user accounts as soon as they are no longer needed and periodically review user accounts for necessity.

District response:
The District has implemented an employee checklist for when an employee leaves employment with the District. This checklist was developed collaboratively with our Human Resources Department, the Director of Information Technology, and the Superintendent's Office. In addition, the District has implemented a regular review of all vendor support accounts.

Comptroller recommendation number two:
Develop and adopt a written IT contingency plan.

District response:
The District prides itself in maintaining a robust network comprised of local and offsite networked infrastructure. As noted in the recommendation, the District is setting up a complete backup redundant process to provide another layer of operational efficiency further. We will continue to develop and update

procedures and policies to enhance an IT contingency plan. Once the board of education approves, the contingency plan will be distributed to all responsible parties.

In conclusion, we once again thank the staff of the comptroller's office for their professionalism throughout the audit process. We appreciated the ability to respond to the audit recommendations, allowing Chittenango Central School to further strengthen its IT policies and procedures. Once confirmation of this submission's acceptance, we will develop our Corrective Action Plan (CAP) with much greater specificity.

Sincerely,

Michael R. Eiffe
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. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We reviewed the District's IT policies and procedures and interviewed the Superintendent, Assistant Superintendent and Director to gain an understanding of the District's IT environment, including management of nonstudent network and local user account access and whether the District had an IT contingency plan.
- We ran a computerized audit script on the District's domain controller on April 11, 2023. We analyzed the script results to obtain information about the District's 578 enabled nonstudent network user accounts, including their permissions, to determine whether they were necessary and appropriate. We compared the 578 enabled nonstudent network user accounts to the active employee list to identify user accounts for former employees and other accounts that may have been unneeded. We followed up with District officials and CNYRIC staff to assess whether the accounts and administrative permissions were needed for certain accounts. For user accounts that were deemed unneeded, we spoke with District officials to determine the date when access to the account was last needed and assessed whether the account was logged into after the date provided. We ran a second computerized audit script on August 9, 2023, to determine whether the identified unneeded network user accounts were disabled.
- We used our professional judgment to select a sample of 12 user computers assigned to 11 District employees whose job duties indicated they regularly accessed or had access to PPSI. We ran a computerized audit script on the 12 user computers on April 11, 2023, and analyzed the results generated by the script to obtain information about the computers' local user accounts, including their permissions, to determine whether they were necessary and appropriate. We also reviewed network user accounts with local administrative permissions on the 12 user computers.

Our audit also examined the adequacy of certain sensitive IT 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 C: Resources and Services

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

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

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

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

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

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/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.ny.gov/local-government/required-reporting

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

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

https://www.osc.ny.gov/local-government

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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief of Municipal Audits

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