New York State Comptroller
THOMAS P. DiNAPOLI

Wheatland-Chili Central School District

Network Access Controls

2023M-7 | June 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Wheatland-Chili Central School District

Audit Objective

Determine whether Wheatland-Chili Central School District (District) officials ensured network access controls were adequate.

Key Findings

District officials did not ensure that network access controls were adequate. As a result, there is a significant risk that network resources, financial data and student information could be inappropriately altered, accessed or used. In addition to the sensitive network access control weaknesses that were communicated confidentially to officials, District officials did not:

- Comply with Board policies to help ensure adequate network access controls were in place, including a comprehensive written information technology (IT) disaster recovery plan and employee IT security awareness training.
- Review and assess the need for 292 inactive network user accounts.

In addition, the District did not have a written agreement with BOCES to itemize and define all IT services and responsibilities, including network access and server hosting, and related controls, costing approximately $120,000.

Key Recommendations

- Establish and enforce adequate written policies and procedures, including a comprehensive IT disaster recovery plan, and provide IT security awareness training to employees.
- Disable unnecessary network user accounts, modify network access timely and periodically review network user accounts for necessity.
- Work with BOCES to develop a written agreement with a detailed list and explanation of services and responsibilities.

District officials generally agreed with our findings and indicated they plan to initiate corrective action.

Background

The District serves the Towns of Chili, Wheatland and Brighton in Monroe County and the Town of Caledonia in Livingston County.

The District is governed by an elected seven-member Board of Education (Board) responsible for managing and controlling educational and financial 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 administration under the Board's direction.

The District's Director of Technology (IT Director) manages IT operations including network access controls.

The District contracts with Monroe One Board of Cooperative Educational Services (BOCES), using a cross-contract through Monroe 2-Orleans BOCES, to provide IT services such as network server hosting, virtual hardware hosting and related technical support.

Quick Facts

Enabled Network User Accounts	
Student	772
Staff	332
Service	108
Shared	42
Total	1,254

Audit Period

July 1, 2020 – July 21, 2022

Network Access Controls

The District relies on its network access for maintaining financial, personnel and student records, Internet access and email, much of which contain personal, private and sensitive information (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 or entities. If network access is disrupted or compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and/or rebuild. While effective network access controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized network use, access and loss.

Until June 2021, the District subscribed to the BOCES Managed IT Service, and used BOCES as its IT Department, responsible for managing all network services and IT assets. In June 2021, the District hired an IT Director to manage IT operations, including network access controls, and contracted with BOCES to provide specific IT services such as network server hosting, virtual hardware hosting and related technical support.

What Policies and Procedures Should the School District Board Adopt to Help Ensure Adequate Network Access Controls?

Network access control policies should describe the tools to use and procedures to follow to help protect the network and the data it contains, define appropriate user behavior when accessing the network and explain the consequences of policy violations.

To minimize the risk of unauthorized network access, a school district board (board) should adopt policies to help actively manage network user accounts, including their creation, use and dormancy, regular monitoring to ensure they are appropriate and necessary, and timely disabling when no longer needed. Additionally, the board should adopt written policies that address other IT topics that could impact network access controls including, but not limited to, Internet and computer use, passwords, remote access, use of removable storage devices, IT security training and IT asset inventories.

School district officials should also develop a comprehensive written IT disaster recovery plan that specifies the procedures and technical measures for restoring necessary network operations after an unplanned disruption (e.g., system failure caused by an inadvertent employee action, power outage, ransomware or other type of malware infection, or a natural disaster such as a flood or fire). The plan should address how users will access the network or its data as quickly and effectively as possible to maintain school district operations and should be distributed to all responsible parties and periodically tested.

A board should ensure that school district officials monitor for compliance with and enforce the policies and develop and implement any required procedures – generally referred to as administrative regulations and numbered to coincide with related policies – to supplement and implement the policies. Without establishing, monitoring for compliance with and enforcing comprehensive written policies and procedures that explicitly convey a school district's network access controls, school district officials cannot ensure users are aware of their responsibilities for helping to protect the network and data it contains from unauthorized use, access and loss.

Officials Did Not Develop or Enforce Adequate Network Access Control Policies and Procedures

The Board adopted several information technology policies including: Information Security Management, Data Networks and Security Access, Staff Use of Computerized Information Resources and Email Use. However, we found that the Board did not enforce the policies or ensure that District officials developed adequate written procedures to effectively implement the policies. Therefore, District officials did not ensure that network access controls were adequate.

Network User Accounts – The Board did not ensure that District officials developed procedures to add or disable network user accounts, as required in its Data Networks and Security Access policy. In practice, the IT Director is responsible for adding and removing network access when he receives an email request (or sometimes paper onboarding forms) from the District Clerk. The IT Director stated that managers send him email requests when they need him to modify an individual's access to the network and specific software. The IT Director does not periodically review a list of current authorized network users and their level of access to the network.

Because the District did not have written detailed procedures for adding or revoking network access permissions and regularly reviewing enabled network user accounts, many unneeded network user accounts[1] went unnoticed until after our audit inquiry and could have been used as entry points for attackers to access the District's network resources accessible through these accounts.

District officials did not enforce the District's policy and regulation on acceptable staff use of IT resources. …

Computer Use – District officials did not enforce the District's policy and regulation on acceptable staff use of IT resources which include accessing the District's network. The policy states that personal use of social media during District time or on District-owned equipment is prohibited. Additionally, the District's regulation[2] prohibits the use of the District's computer system for other than school-related

1 See "District Officials Did Not Adequately Control Network User Account Access."
2 6470R – Last approved May 1, 2012, as required by, and to implement, the terms of Policy 6470

work or activities. Furthermore, the policy and regulation require all staff to receive a copy of the District's policies on computer use and sign an acceptable use agreement form before obtaining a computer account on the District's network. The email use policy includes the same requirement and requires staff to annually acknowledge the policy and regulation on staff computer use.

We reviewed the web browsing histories on 11 District computers for evidence of personal use and found that District employees' assigned computers were used to visit various websites that did not appear to be for District purposes, including social networking, online shopping, car dealership, real estate, online gaming, job searching, video and music streaming and other entertainment websites. Furthermore, we conducted a detailed review of the shared folders of the users of the same 11 computers and a more cursory review – using key-word searches – of the data for all other users and found that some of the shared folders contained potential personal content including music, photos and tax returns. The IT Director looked at the content in some of the folders during our discussions and confirmed that it appeared personal.

Additionally, the District did not require employees to sign an acceptable use agreement form. In fact, officials stated they were unaware of the regulation requiring the form, which is concerning, in addition to the fact that the requirement is also included in the staff computer use and email use policies.

…[T]he District did not require employees to sign an acceptable use agreement form… officials stated they were unaware of the regulation requiring the form. …

Passwords – The District's Data Networks and Security Access policy is a control which entrusts the Superintendent or his/her designee to develop password standards and controls for all users including, but not limited to, how to create passwords and how often such passwords should be changed by users to ensure security of access to the District's network. District officials have not developed a written regulation on the requirements for password standards.

Remote Access – The District's Data Networks and Security Access policy is a control which entrusts the Superintendent or his/her designee to determine how, and to whom, remote access should be granted to the District's network. The policy requires written agreements be obtained from remote access users that establish the District's needs and expectations, as appropriate, and provides for the monitoring and control of such remote access. District officials have not developed procedures to establish those vital controls and determine how and to whom remote access should be granted and have not obtained written agreements from remote access users.

Use of Removable Storage Devices – The Board and District officials did not develop specific policy and procedural guidance for whether staff or students were permitted to use personal or District-owned mobile storage devices, such as USB flash drives, on devices which connect to the District's network. Such guidance should address security procedures to compensate for the use of

personal devices, if allowed, such as requiring all mobile storage devices use an approved method of encryption and/or password to protect the District's network and data if it was lost or stolen.

IT Security Training – The Board did not ensure that District officials developed procedural regulations to provide staff with periodic IT security training on the proper and effective use of the District's computer system, including accessing its network, as required by the staff computer use and email use policies. To minimize the risk of unauthorized network access and misuse or loss of data and PPSI, periodic IT security awareness training should be scheduled to explain District policies and procedures and communicate the rules of proper behavior for using the Internet and IT systems and data.

District officials did not provide employees with IT security awareness training to help ensure they understand the IT security measures and controls that were designed to help safeguard access to the District's network and the data contained therein.

Inventory – The Board did not ensure that District officials developed formal procedures for maintaining detailed IT asset inventory records, as required by the Data Networks and Security Access policy. The policy requires procedures for tagging IT assets when purchased, relocating assets, updating inventory lists, performing periodic physical inventories and investigating any differences, in an effort to know the location and control the security of all IT assets to help prevent unauthorized or malicious access to these assets, or to the District's network using these assets. The detailed inventory record should include a description of each item, including the make, model and serial number; the name of the person to whom the equipment is assigned; the physical location of the asset (and any relocations or reassignments); and relevant purchase information including acquisition date and cost.

District officials did not maintain a comprehensive inventory of physical IT assets. The IT Director told us that BOCES-owned equipment is tracked by BOCES and recorded in the resource manager program. However, the IT Director was aware that the system was not kept up to date. In addition, they did not have adequate controls over or inventory records for other IT assets, especially those that are not currently assigned to specific users. The IT Director described instances when he found unused equipment piled up in random locations. The lack of an adequately implemented inventory tracking system exposes untracked and potentially unsecured assets to increased risk of unauthorized access by malicious users. The District recently purchased its own IT inventory system.

During our May 9, 2023 exit conference, the IT Director told us that he has fully implemented the IT asset inventory system. He demonstrated the system, showed us how he can now look up or run reports for all types of equipment with

status and location, or all equipment assigned to specific staff or students, and provided a sample inventory report – of all laptops assigned to elementary school staff and students.

Disaster Recovery Plan – The Board's Information Security Management policy and Data Networks and Security Access policy are controls which require the Superintendent or designee to develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations to ensure continuous critical IT services, such as access to the District's network, in the event of any sudden, catastrophic event, including fire, computer virus or deliberate or inadvertent employee action. However, the District does not have a comprehensive IT continuity or disaster recovery plan for its IT operations. On our inquiry, the IT Director contacted BOCES to request its IT disaster recovery plan and was provided a copy of its emergency response plan. We found the plan was generic and did not provide necessary information specific to the District to help enable the recovery of access to the District's network after an unexpected incident.

While network access policies and procedures are controls which do not guarantee the safety of the network or the electronic information contained therein, without developing, monitoring for compliance with and enforcing these policies and procedures, the District has an increased risk that its network hardware, software and data, including PPSI, may be exposed, damaged or lost through inappropriate network access and use. Also, when officials do not have an appropriate IT disaster recovery plan in place, the District is at risk of disruptions in District operations and could suffer unnecessary and preventable losses.

How Should School District Officials Control Network User Account Access?

School district officials are responsible for implementing network access controls that should include restricting network user account access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets on the network are secure from unauthorized access, use, modification and/or loss.

Network user accounts provide access to network resources which may include financial and employee data. If not adequately managed, unnecessary network user accounts may not be detected and disabled in a timely manner. Also, unneeded accounts are additional entry points for attackers to potentially gain network access and then attempt to view PPSI inappropriately, make unauthorized changes to official District records or deny legitimate access to electronic information when needed.

…[Un]needed accounts are additional entry points for attackers to potentially gain network access. …

To minimize the risk of unauthorized network access, misuse and loss, officials should actively manage network user accounts, including their creation, use and dormancy. Officials should disable unnecessary network user accounts as soon as there is no longer a need for them, and regularly monitor active accounts to ensure all are appropriate and authorized.

A service account is an account created for the sole purpose of running a particular network or system service or application (e.g., backups). Service accounts should be limited in use as they are not linked to individual users and therefore, hinder the ability of officials to identify the actions of specific users. Officials should routinely evaluate the need for service accounts and disable those that are not related to a current school district or system need.

Shared network user accounts are accounts with a username and password that are known and used by two or more users. Shared accounts are often used to provide access to guests and other temporary or intermittent users (e.g., substitute teachers and third-party vendors). Because shared accounts are not assigned to an individual user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. Therefore, officials should limit the use of shared network user accounts.

Officials Did Not Adequately Control Network User Account Access

Due to inadequate network access controls, the District had unneeded user accounts that remained enabled on its network. We examined all 1,254 enabled network user accounts (772 student accounts, 332 individual nonstudent accounts, 108 service accounts, and 42 shared accounts) to determine whether accounts were necessary and appropriate. We found 292 enabled accounts that had not been recently used.

…232 individual network user accounts…had not been used within the last six months…over 40 percent of these accounts were not used since 2018, the oldest since 2013.

Individual Student and Nonstudent Network User Accounts – We inquired with the IT Director about 232 individual network user accounts that had not been used within the last six months prior to our audit testing. These included accounts for 100 students, 49 BOCES employees, 38 substitutes, 31 staff, seven vendors and seven unidentified users. The IT Director, new to his position, was unaware which, if any, of the accounts were still needed. For additional perspective, over 40 percent of these accounts were not used since 2018, the oldest since 2013.

The District Clerk or BOCES did not consistently share or act on notifications of employee or student departure before the IT Director position was created. The IT Director told us he planned to review the accounts and determine which are still in use. He said he would disable the unneeded accounts and then delete them after 30 days if he receives no complaints from users needing to access the disabled accounts. However, any unneeded accounts, particularly those for former students or staff, should have been disabled as soon as the individuals separated from the District or no longer needed network access.

During our September 26, 2022 findings meeting, the IT Director stated that, after we helped him identify which network user accounts were for BOCES employees who were no longer assigned to the District, he deleted those accounts. He has addressed some of the former employee and student accounts as well and will continue those efforts. However, he did not maintain a record of the accounts he addressed and deleted.

Service and Shared Network User Accounts – The District had 108 service and 42 shared network user accounts. Sixty of these accounts had not been used within the last six months prior to our audit testing. The IT Director reviewed the accounts and stated that 66 service accounts were created for a BOCES-hosted service (four of the 66 were not used in the last six months). However, he said those network user accounts were no longer needed as of May 2022, and he will need to follow up with BOCES to determine who can delete those accounts.

The IT Director was unaware which, if any, of the remaining 84 accounts were still needed, and said he planned to determine which ones are necessary and which ones can be disabled and deleted. As of September 26, 2022, he stated that he disabled and deleted some of the service accounts and will continue those efforts. However, he did not maintain a record of what accounts he addressed and whether they were retained, disabled or deleted.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could possibly be used to inappropriately access and view PPSI. For example, we noted that at least five of the inactive staff accounts had access to student PPSI. When network user accounts are not used or regularly reviewed, compromised accounts may not be detected in a timely manner.

After our May 9, 2023 exit conference, the IT Director provided additional documentation that he had reviewed all 108 service accounts and deleted all but 37 accounts, which were still needed for active software applications. He indicated that he had also cleaned up inactive student accounts but was still working on shared accounts and unused staff accounts.

Why Should the School District Define the Expected Services from Its IT Service Provider?

School district officials should ensure they have qualified IT personnel to help ensure adequate network access controls. This can be accomplished by using school district employees, an IT service provider or both. To protect the school district's network and avoid potential misunderstandings, school district officials should have a written agreement with the school district's IT service provider that clearly identifies the school district's needs and service expectations, and how

the IT service provider will meet them. The agreement must include provisions relating to the confidentiality and protection of PPSI of students, teachers and principals.

Written expectations help ensure there is mutual understanding between the school district and its service provider for the nature and required level of services to be provided. School district officials should monitor the work performed by the IT service provider to ensure the school district receives the required, expected services, and does not pay for services it does not require or receive. The agreement should be reviewed by knowledgeable IT staff, legal counsel, or both, and be periodically reviewed, especially if the IT environment or needs change significantly.

Officials Did Not Adequately Define the Expected Services of the District's IT Service Provider

The District engaged BOCES to provide various IT support and services costing over $480,000. These services included equipment, software and support services that were pass-through payments to vendors, as well as server hosting and support for network access controls – which cost approximately $120,000 for the 2021-22 and 2022-23 fiscal years. District officials did not have a formal agreement with BOCES to set defined written expectations and identify the roles, responsibilities and specific services BOCES was providing.

The lack of stated responsibilities and procedures for network access controls can contribute to confusion over who has responsibility for the various aspects of the District's network access control management, which could put the District's network resources and data at greater risk for unauthorized access, misuse or loss. The IT Director, who was completing his first year with the District, expressed a strong need for a detailed formal agreement, and concerns that he did not know for certain which functions and duties BOCES was performing, or how, and which were his responsibility. During our September 26, 2022 findings meeting, the Superintendent, along with the Board President and School Business Official, also acknowledged this concern that has resulted from common and long-standing BOCES practices.

What Do We Recommend?

The Board should:

1. Adopt more detailed written IT policies or require officials to develop written procedures including detailed guidance for managing network user account access controls, use of removable storage devices, employee IT security training and IT asset inventory.

2. Ensure officials enforce compliance with adopted policies and procedures including those for computer use, passwords, remote access and email use.

The Board and District officials should:

3. Execute a detailed written agreement with BOCES that sets expectations and describes the District's specific needs for network access control support and other IT services, the roles and responsibilities of each party and the services that will be provided.

District officials should:

4. Develop and implement written procedures for managing network user account access controls, computer use, passwords, remote access, use of removable storage devices, IT security training and IT inventory.

5. Develop a comprehensive written IT contingency or disaster recovery plan that provides specific guidance for the protection of IT assets and data on the District's network against loss or destruction and steps to resume operations after a potential disaster. Ensure the plan is periodically tested and updated.

The IT Director should:

6. Become familiar with and enforce compliance with District policies and procedures or regulations.

7. Disable network user accounts as soon as there is no longer a need for them, and regularly review and update network user accounts for necessity and appropriateness.

Appendix A: Response From District Officials

Wheatland-Chili
CENTRAL SCHOOL DISTRICT

District Office
13 Beckwith Avenue | Scottsville, NY 14546
P 585.889.4500 F 585.889.6284
www.wheatland.k12.ny.us

Lynda Quick, Esq.
Superintendent

May 31, 2023

To Whom It May Concern:

The Wheatland-Chili Central School District had an Instructional Technology Audit performed by the New York State Office of the State Comptroller between July 1, 2020, and July 21, 2022. The District was provided with the draft public report on April 25, 2023, and a revised draft on May 22, 2023. This audit focused on network access controls and the potential risk that network resources, financial data and student information could be inappropriately altered, accessed, or used.

The public report conveyed key findings and recommendations. They are:

- The District needs to comply with Board policies to help ensure adequate network access controls are in place, including a comprehensive written information technology (IT) disaster recovery plan and employee IT security awareness training.
- The District needs to review and assess the need for inactive network user accounts.

In addition, it is recommended that the District enhance the agreement with BOCES to itemize and define IT services and responsibilities, including network access and server hosting and related controls.

Overall, the District understands these key areas and is in agreement with the methodology used to realize these recommendations. While the District has completed disaster recovery drills, the District will work to develop a comprehensive written information technology (IT) disaster recovery plan and security awareness training. The District, since this audit was performed, has disabled inactive network user accounts, and will develop a process to monitor such accounts and access going forward.

Finally, the Monroe Regional Information Center, one of 12 regional information centers across the state, is a resource to the 19 component school districts in Monroe County New York. They work with and help guide Wheatland-Chili in the above noted areas. We do have a Co-Ser agreement for the purchase of services from Monroe Regional Information Center, but we will work to improve the specifications the audit report recommends.

Further, the District intends to create a formal corrective action plan to ensure all of the recommendations contained within the audit are appropriately addressed.

Sincerely,

Lynda Quick, Esq.
Superintendent

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 the District's IT policies and procedures and the BOCES emergency response plan and interviewed District and BOCES officials to gain an understanding of IT operations, specifically those related to network access controls.
- We examined network user accounts using a computerized audit script run on March 29, 2022, April 8, 2022 and again on April 14, 2022. We reviewed the network user accounts and compared them to current employee and student lists to identify inactive and possibly unneeded network user accounts.
- We followed up with District officials on potentially unneeded network user accounts.
- We reviewed web browsing history on 11 judgmentally selected computers. Our selection was based on the ability of the computers' primary users to access PPSI.
- We ran a computerized audit script on the District's shared file server on June 22, 2022 to review for necessity of network access permissions and indications of personal use.
- We assessed the adequacy of the District's documentation for requested BOCES IT services and determined the cost of those services paid for the 2020-21 school year.

Our audit also examined the adequacy of certain sensitive network access 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.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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties