REPORT OF EXAMINATION | 2022M-93

York Central School District

Network Access Controls

OCTOBER 2022

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

Contents

Report Highlights

York Central School District

Audit Objective

Determine whether York Central School District (District) officials ensured network access controls were adequate.

Key Findings

District officials did not ensure that network access controls were adequate. Specifically:

- District officials did not comply with Board policy to ensure adequate network access control procedures were established including a comprehensive written disaster recovery plan.
- The District had 139 unneeded network user accounts and one account with unnecessary network administrative permissions.
- Officials paid $360,896 for information technology (IT) services in 2020-21 without documenting the specific services the IT vendor was contracted to provide.

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

Key Recommendations

- Ensure officials enforce compliance with the data, network and security access policy.
- Disable unneeded network user accounts in a timely manner, and regularly review user accounts for necessity and appropriateness.
- Set written expectations for the District's specific IT service needs.

Background

The District serves the Towns of Leicester and York in Livingston County, and the Town of Perry in Wyoming County.

The District is governed by a seven-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 responsible for District administration.

The District pays the Genesee Valley Board of Cooperative Educational Services (BOCES) for IT services provided by the Wayne-Finger Lakes BOCES through a cross-contract.

The District's Director of IT (IT Director) is responsible for managing IT operations including network access controls with assistance from a technology support assistant and Wayne-Finger Lakes BOCES staff.

The IT Director started in the position effective July 1, 2021 and prior to that was a technology support assistant with the District.

Quick Facts

Enabled Network User Accounts	
Student	905
Individual Non-Student	216
Service	14
Shared	27
Total	1,162

Audit Period

July 1, 2020 – May 12, 2022

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

Network Access Controls

The District relies on its network for Internet access, email and maintaining financial, student and personnel records, 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 compromised or disrupted, 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 these systems, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

What Policies and Procedures Should the 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.

A school district board (board) should adopt written policies that address topics including but not limited to user accounts, passwords, remote access and audit trails (records of activity that can include the accounts used to access the network, the times and dates of the access and what activity occurred). Officials should also develop a comprehensive written disaster recovery plan that addresses, in part, the procedures and technical measures for restoring necessary network operations after an unplanned disruption (e.g., inadvertent employee action, flood or fire). The disaster recovery plan should address how users will access the network or its data as quickly and effectively as possible to maintain business operations, be distributed to all responsible parties and periodically tested. A board also should ensure that officials monitor and enforce the policies and develop any required procedures to supplement the policies.

Without comprehensive written policies and procedures that explicitly convey a school district's network access controls, officials cannot ensure users are aware of their responsibilities for helping to protect the network and the 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 a written data, network and security access policy, but did not ensure that officials enforced compliance with the policy requirements. The policy required the Superintendent, or his designee, to manage (grant, change,

terminate) user access rights and permissions to the network; develop password standards; develop necessary security procedures (such as to authorize, monitor and control remote access); and establish procedures for a periodic review of the network audit trail.

District officials did not establish certain procedures as required by the policy. Without these additional procedures, the policy did not adequately address these areas. The Superintendent did not provide an explanation for why they were not previously developed and told us that they were in the process of developing written procedures. We found officials did not:

- Adequately manage user accounts for the network including establishing adequate written procedures to add or disable user accounts or grant or change user permissions.
- Develop written standards for network password security prior to the start of our audit fieldwork. Officials developed written password standards and provided them to us in January 2022, but they were not adequate.
- Develop written procedures for adequately authorizing, monitoring and controlling remote access. The new password standards document contained a brief section on controlling remote access but did not provide procedures for granting or monitoring remote access.
- Establish written procedures for audit trail review and did not review network audit trail activity for indications of unauthorized or inappropriate network access activity.

While network access control policies and procedures do not guarantee the safety of the network or the electronic information contained therein, without these policies and procedures the District has an increased risk that its hardware, software and data, including PPSI, may be exposed, damaged or lost through inappropriate access and use. Also, when officials do not regularly review network audit trails, they may not detect unauthorized or inappropriate activity within the network in a timely manner.

Officials Did Not Develop an Adequate Disaster Recovery Plan

The policy also required the Superintendent, or his designee, to develop a disaster recovery plan. However, officials did not develop an adequate disaster recovery plan to help enable the recovery of network operations to provide access after an unexpected disruption. The District's disaster recovery plan consisted of a cybersecurity incident response plan (cybersecurity plan) that adequately addressed cybersecurity incidents; however officials did not ensure that the cybersecurity plan was periodically reviewed, distributed and tested. In addition, the cybersecurity plan did not include other necessary elements for business

continuity that should be included in an adequate comprehensive disaster recovery plan, including:

- Prioritizing mission-critical processes and services,
- Details on how the plan will be periodically tested, or
- How users will continue to work during a disruption.

The IT Director and Business Official were initially unaware of the written cybersecurity plan and the IT Director told us that he did not know what he would do if there was a disaster. The Superintendent was aware of and provided the cybersecurity plan, but without a comprehensive written disaster recovery plan properly distributed to all responsible parties and periodically tested for efficacy, District officials have less assurance that individuals will react quickly and effectively to maintain business continuity.

Without a comprehensive disaster recovery plan, the District is at risk of disruptions in business operations after an unplanned disruption and could suffer unnecessary and preventable losses.

If not adequately managed, unnecessary user accounts may not be detected and disabled in a timely manner.

How Should Officials Manage Network User Account Access?

School district officials are responsible for 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 use, modification and/or loss.

Network user accounts provide access to network resources which may include financial and employee data and should be actively managed to minimize the risk of unauthorized access and misuse. If not adequately managed, unnecessary user accounts may not be detected and disabled in a timely manner. Also, unneeded accounts could be entry points for attackers to potentially access and view PPSI inappropriately, make unauthorized changes to records or deny legitimate access to electronic information when needed.

To minimize the risk of unauthorized access, misuse and loss, 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. Officials should disable unnecessary user accounts as soon as there is no longer a need for them.

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, may have reduced accountability. 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 user accounts are accounts with a username and password that are shared among 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 user accounts.

To help ensure individual accountability, each user should have and use their own user account, when possible. When shared user accounts are provided for temporary work or guests, the accounts should have an expiration date and automatically terminate access after a designated, authorized time period.

Generally, a network administrative account has permissions to monitor and control a network, connected computers and certain applications, such as adding new users and changing user passwords and permissions. Additionally, a user with administrative permissions on a network can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, officials should limit network administrative permissions to those users who need them to complete their job duties and functions.

Officials Did Not Adequately Manage Network User Account Access

District officials did not adequately manage network user account access. As a result, the District had enabled and unneeded, unused and shared user accounts and permissions.

We examined all 1,162 enabled network user accounts (905 student accounts, 216 individual nonstudent accounts, 14 service accounts, and 27 shared accounts) to determine whether accounts were necessary and appropriate.

Unneeded Individual Network User Accounts – Upon our request, District officials reviewed the 383 individual network user accounts (322 student accounts and 61 nonstudent accounts) that had not been used in at least six months and disabled 110 of the 383 accounts (29 percent) and 10 additional user accounts with activity in the past six months because they were no longer needed. This included three individuals that the IT Director initially told us were current employees or providers, but upon discussions with other District employees, we determined were no longer with the District. The disabled accounts included those for 60 former students who had graduated, 57 former employees, BOCES staff or others no longer employed by or working at the District and three current employees.

These accounts should have been disabled as soon as the individuals graduated or separated employment or service, or no longer needed network access. However, they remained enabled for much longer than necessary. For example, we identified 15 enabled user accounts of former employees who had not been employed by the District in more than three years. Generally, these accounts were still enabled because there were not adequate procedures to follow for disabling accounts and the IT Director did not perform an adequate periodic review of authorized users and their levels of access to the network. The IT Director told us that our inquiry helped identify unneeded accounts.

The IT Director determined the remaining 271 inactive user accounts (262 students, 11 individual nonstudent accounts) were needed. However, this included one former employee's network user account. The IT Director told us that this user account was still enabled to obtain information from the former employee's email and they planned to disable it at the end of the 2021-22 school year. The IT Director also told us that the other inactive but still enabled accounts were generally for students and staff who usually do not access the network but should have accounts to do so if needed.

Unneeded Service and Shared Network User Accounts – There were 27 shared and 14 service network user accounts. Upon our request, District officials reviewed these accounts and told us they disabled 13 shared and five service accounts because they were not needed. Overall, 44 percent of service and shared network user accounts were unneeded. Of these, one was a shared account used by the District's technology staff as a test account and they plan to re-enable it on an as-needed basis. Generally, these accounts were still enabled because there were not adequate procedures to follow for disabling accounts.

In total, officials disabled 138 (12 percent) of the 1,162 enabled network user accounts because they were not needed. Unneeded 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. When network user accounts are not used or monitored, compromised accounts may not be detected in a timely manner.

Unnecessary Network Administrative Permissions – There were 14 user accounts with network administrative permissions (11 service or shared accounts, two IT staff user accounts and one teacher's user account). The IT Director told us that he removed administrative permissions from the teacher's user account because the teacher did not require these permissions. The IT Director was unable to explain why the teacher was given administrative permissions. The administrative permissions for the remaining 13 user accounts were necessary at the time of testing. The IT Director told us that three of these user accounts were no longer needed as of February 2022.

When users' accounts have unneeded network administrative permissions, they could potentially 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.

District officials did not set defined written expectations with Wayne-Finger Lakes BOCES. …

Why Should a District Define the Expected Services from its IT Service Provider?

To protect the school district's network and avoid potential misunderstandings, officials should have written expectations with the school district's IT service provider that establish the school district's needs, clearly identify the IT service provider's roles and responsibilities and set the school district's service expectations.

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. Officials should monitor the work performed by the IT service provider to ensure the school district receives required, expected services.

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

The District engaged Wayne-Finger Lakes BOCES (paid through Genesee Valley BOCES) to provide network support and various services, including support for network access controls. District officials did not set defined written expectations with Wayne-Finger Lakes BOCES to identify the roles, responsibilities and specific services the District paid for. For perspective, officials paid Genesee Valley BOCES $360,896 for all IT support and services in 2020-21.[1]

While officials chose Wayne-Finger Lakes BOCES services by selecting certain items from a list of available Wayne-Finger Lakes BOCES IT services, District officials did not have this documentation available and these lists generally do not provide detailed explanations of the services or costs. As a result, officials do not know what specific services they paid for or the specific services provided and were unable to determine whether they were appropriately billed for these services. In addition, officials do not know if they were receiving the best value for similar goods and services offered by other IT service providers.

Furthermore, officials did not have procedures in place to monitor and review the work performed by Wayne-Finger Lakes BOCES staff. Therefore, officials could not ensure the District's network was adequately safeguarded.

[1] The District's financial software did not break down costs in detail to obtain the specific cost for only those services directly related to network access controls.

As a result, the District and Wayne-Finger Lakes BOCES did not have stated responsibilities and procedures for network access controls. This 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 resources and data at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Ensure officials enforce compliance with the data, network and security access policy.

The Board and District officials should:

2. Set written expectations with Wayne-Finger Lakes BOCES that describe the District's specific needs for network support and services, the roles and responsibilities of each party and the services that will be provided.

District officials should:

3. Develop adequate written procedures for managing network user account access controls, passwords, remote access and reviewing network audit trails.

4. Ensure that the cybersecurity plan is distributed to all individuals responsible for implementing the plan and tested and develop a more comprehensive written disaster recovery plan to adequately address non-cybersecurity incidents and other IT contingency plan items.

The IT Director should:

5. Perform a periodic review of the network audit trail for indications of unauthorized or inappropriate network access activity.

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

Appendix A: Response From District Officials

York Central School

David M. Furletti, *Superintendent*

Paul J. Liess, Jr, *School Business Official*

Aubrey L. Krenzer, *Director of Curriculum & Instruction*

GOLDEN KNIGHTS

Lindsey M. Peet, *Middle/High School Principal*

Edward J. Orman, Interim *Elementary School Principal*

Ameigh J. Coates, *Pupil Personnel Services Director*

Date: September 13, 2022

Re: Response to the Network Access Controls Report

Thank you for the opportunity to respond as we value working together to improve our systems. This letter is in response to the findings of your report and to ensure you are aware of the steps that the York Central School District has been conducting to ensure network safety. YCSD continues to monitor and have Network Audits along with addressing concerns that may arise from any audit.

The District has contracted and continues to work with WFL BOCES (Edutech) on the network access control procedures and the comprehensive written disaster recovery plan, as well as self-audited review internally prior to this audit occurring. York Central School District was aware of these concerns and has been addressing these findings. While the district has completed approximately 90% of the Disaster Recovery Plan, this is an on-going work in progress with the ever changing need in technology.

See Note 1 Page 10

With respect to the findings of unneeded network user accounts and permissions; the district was aware of this from the previous self-requested audit with Edutech. York Central School District has been reviewing accounts and removing the unneeded accounts, as well as, reviewing the permissions of the users. As employees change the accounts and permissions will continue to be maintained and updated.

See Note 1 Page 10

Regarding, the findings with the Information Technology (IT) Services invoices without specific services itemized. The invoices that are discussed in the report are referring to the monthly BOCES billing, and is associated to the Edutech line item. The district requests these services and contracts through Edutech through SA-8, which both the district and Edutech have copies of these signed and approved agreements. The invoices summarizes the total monthly cost, but all of the supporting documentation regarding these expenses have been approved with signed contracts through WFL BOCES.

See Note 1 Page 10

The district appreciates the Office of the State Comptroller's opinions and recommendations. The district has pro-actively been resolving these finding in a previously completed audit the school district requested. The school district intends to focus on and continue to improve the operations of the District's Network, Access, and Controls.

See Note 1 Page 10

Respectfully,

David Furletti, Superintendent of Schools

PO BOX 102 • 2578 Genesee Street • Retsof, NY 14539 • Phone: 585-243-1730 • Fax: 585-243-5269 • www.yorkcsd.org

The York Central School District rises to the challenges and provides opportunities for empowerment, exploration, growth and success.

Appendix B: OSC Comment on the District's Response

Note 1

Although District officials were asked if any IT audits or other IT engagements were ongoing or completed, District officials did not share that a BOCES audit or a District "self-audit" was conducted. Officials also did not provide any documentation to support any action taken to mitigate the risks the engagement identified. Had the risks been mitigated, we would not have identified the same findings. In addition, the audit did not criticize the monthly BOCES billing process. The audit found that District officials did not set defined written expectations with Wayne-Finger Lakes BOCES. Officials did not identify the roles, responsibilities and specific services BOCES was contracted to provide and for which the District paid for. Furthermore, the IT Director and Business Official told us that they did not have a BOCES IT contract available for us to review.

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 reviewed the District's IT policies, procedures and the cybersecurity incident response plan and interviewed District and Wayne-Finger Lakes BOCES officials to gain an understanding of IT operations and controls, specifically those related to network access controls.
- We examined network user accounts and permissions using a computerized audit script run on December 14, 2021. We reviewed the network user accounts and compared them to current employee lists and student classes to identify inactive and possibly unneeded network user accounts and permissions.
- We followed up with District officials on potentially unneeded accounts and permissions.
- We assessed the adequacy of the District's documentation for requested Wayne-Finger Lakes BOCES IT services and determined the cost of those services paid in 2020-21.

Our audit also examined the adequacy of certain 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.

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

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

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