REPORT OF EXAMINATION | 2021M-79

Penn Yan Central School District

Network Access Controls

SEPTEMBER 2021

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

Contents

Report Highlights

Penn Yann Central School District

Audit Objective

Determine whether Penn Yan Central School District (District) officials ensured network access controls were secure.

Key Findings

District officials did not ensure that the District's network access controls were secure.

Officials did not:

- Regularly review network user accounts and permissions to determine whether they were appropriate or needed to be disabled. As a result, we identified 1,094 unneeded user accounts and six user accounts with unnecessary administrator permissions.
- Enter into a service level agreement (SLA) with the District's Information Technology (IT) service provider to clearly identify the provider's responsibilities and services to be provided.

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

Key Recommendations

- Regularly review network user accounts and disable those that are unnecessary.
- Develop an SLA to address the District's specific needs and expectations for IT services.

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

Background

The District serves the Towns of Barrington, Benton, Jerusalem, Milo, Potter and Torrey in Yates County, Geneva and Seneca in Ontario County and Pulteney in Steuben County.

The District is governed by a nine-member Board of Education (Board) responsible for managing and controlling financial and educational affairs.

The Superintendent of Schools is the chief executive officer and responsible for District administration.

The District's Technology Manager (Manager) oversees day-to-day IT operations. Two District computer aides and Wayne-Finger Lakes Board of Cooperative Educational Services (BOCES) staff assist with these duties.

The District relies on its IT assets for Internet access, email and maintaining confidential and sensitive financial, student and personnel records.

Enabled Network User Account Quick Facts	
Student	1,823
Generic	76
Staff	336
Total	2,235

Audit Period

July 1, 2019 – May 7, 2021

Network Access Controls

Why Should Officials Manage Network User Accounts and Permissions?

District officials are responsible for restricting network user 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 are secure from unauthorized use and/or modification.

Network user accounts provide users with access to network resources and should be actively managed to minimize risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers because the accounts could be used to inappropriately access and view personal, private and sensitive information (PPSI),[1] make changes to the records or deny access to electronic information.

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

When user accounts are no longer needed, they should be disabled in a timely manner.

Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. A shared network user account is an account with a username and password that is shared among two or more people. Shared accounts are often used to provide access to guests and temporary or intermittent IT users (e.g., substitute teachers and third-party vendors) and automated processes (e.g., backups and testing).

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

Additionally, any program that a user with administrative permissions runs will inherently run with the same permissions. For example, if malicious software installed itself on a computer, it would run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of network or computer compromise and/or data loss.

1 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.

Officials Did Not Adequately Manage Network User Accounts and Permissions

District officials configured specialized software to automatically manage user accounts on the network. However, officials did not establish policies or procedures to add, disable or change user permissions. As a result, the District had unneeded, unused and shared network user accounts and permissions that were not disabled or monitored. We reviewed all 2,235 enabled network user accounts (1,823 student accounts, 76 generic accounts and 336 nonstudent accounts) for IT security weaknesses.

Unneeded Network User Accounts – We found 1,160 inactive user accounts (51 nonstudent accounts, 50 generic and 1,059 student accounts). District officials reviewed these accounts and other similar accounts upon our request.

District officials told us that they disabled 994 student accounts (55 percent) because 689 student accounts belonged to student in grades five or below who do not log onto the network, and 305 were for students who were no longer enrolled.

Also, officials disabled 52 (15 percent) staff accounts. For example, these accounts included summer school staff, substitutes or temporary staff. However, we found one of the accounts was assigned to an individual who resigned July 23, 2019.

Generic User Accounts – Of the 76 generic or shared network user accounts, 50 were not used in the last six months. Officials reviewed these accounts and disabled 48 (63 percent) unnecessary generic accounts but offered no explanation for why these accounts were unneeded.

In total, officials disabled 1,094 (49 percent) of the 2,235 enabled network user accounts. Unneeded network user accounts can be potential entry points for attackers because they are not monitored or used and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. Also, when the District has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access. In addition, if users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Unnecessary Administrative Permissions – We found 13 accounts with administrative permissions that officials reviewed. Nine of these accounts were generic accounts; eight used for various network functions and one shared by BOCES staff. The remaining four were assigned to IT staff. The IT Manager told us that he disabled six of these user accounts (46 percent) because users did not require these permissions.

When users have unneeded administrative permissions to networks and 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.

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

District officials must ensure they have qualified IT personnel to manage and secure the district's IT environment. This can be accomplished by using district employees, an IT service provider or both. To protect a district's network and avoid potential misunderstandings, officials should have a written SLA with the district's IT service provider that clearly identifies the district's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI.

An SLA is different from a traditional written contract in that it establishes comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement, scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The SLA should be reviewed by knowledgeable IT staff, legal counsel, or both, and be periodically reviewed, especially if the IT environment or needs change significantly.

When users have unneeded administrative permissions to networks and computers, they could make unauthorized changes that might not be detected.

District Officials Did Not Have an SLA With BOCES

District officials provided unrestricted remote access to BOCES staff to provide various IT-related services such as network technical support, IT support and management, Internet filtering, backups and firewall/intrusion detection. However, officials had no policies or procedures in place to monitor and review the work performed by BOCES staff or ensure the District's IT assets and data were safeguarded.

Officials did not provide us with a formal agreement or SLA with BOCES to identify the responsibilities and specific services BOCES provided. Instead, officials chose IT products and services by selecting certain items from a list of available IT services provided by BOCES. However, the list did not provide detailed explanations of the services or the costs. As a result, officials were unable to determine whether they were appropriately billed for these services or if

they were receiving the best value for similar goods and services offered by other IT service providers.

Without a written SLA, the District and BOCES did not have stated responsibilities and procedures for how to resolve any failures in IT controls, such as a service disruption or data breach. This can contribute to confusion over who has responsibility for the various aspects of the District's IT environment, which could put the District's computer resources and data at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Adopt policies and procedures for managing user accounts, including adding, disabling and changing user permissions.
2. Develop an SLA with BOCES to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties. Ensure that the agreement includes measurable performance targets and the related costs.

District officials should:

3. Regularly review and update network user accounts for necessity and appropriateness.
4. Ensure all IT users have and use their own unique network user accounts. Routinely evaluate shared user accounts and disable those that are no longer needed.
5. Assess network user permissions on a regular basis and ensure that network user accounts provide users with appropriate permissions needed to perform their job duties.

Appendix A: Response From District Officials

Howard Dennis
Superintendent of Schools

One School Drive
Penn Yan, NY 14527
315.536.3371
hdennis@pycsd.org
www.pycsd.org

August 19, 2021

Edward V. Grant, Jr.
Chief Examiner
Office of the State Comptroller
Rochester Regional Office
The Powers Building
16 W Main Street, #522
Rochester, NY 14614

RE: Penn Yan Central School District's Network Access Controls Report of Examination 2021-M-79

Dear. Mr. Grant:

This letter is in response to the *Draft Report of Examination: Network Access* Report of Examination for the audited period of July 1, 2019 through May 7, 2021. We had our exit interview on Monday July 19th, 2021.

The Penn Yan Central School District has already begun to implement steps that were outlined in the recommendations portion of the report. These steps and actions will be provided in a full Corrective Action Plan and will be submitted to your office.

The District appreciates the work that was performed by the Office of the State Comptroller when reviewing Penn Yan Central School District's Network Access processes and procedures. We are in agreement with the findings provided after the examination. We prepared our Corrective Action Plan, submitted it for review to the Board of Education, and it was approved at the August 18th, 2021 meeting. The District is committed to protecting sensitive data and appreciates the areas identified as needing improvement.

If there are any questions or concerns, please feel free to reach out at any time.

Thank you.

Sincerely,

Howard Dennis
Superintendent

Howard Dennis
Superintendent of Schools

One School Drive
Penn Yan, NY 14527
315.536.3371
hdennis@pycsd.org
www.pycsd.org

CORRECTIVE ACTION PLAN

Unit Name: Penn Yan Central School District

Audit Report Title: Network Access Controls

Audit Report Number: 2021M-79

For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed.

Audit Findings:

District officials did not ensure that the District's network access controls were secure.
Officials did not:

- Regularly review network user accounts and permissions to determine whether they were appropriate or needed to be disabled.
- Enter into a service level agreement (SLA) with the District's Information Technology (IT) service provider to clearly identify the provider's responsibilities and series to be provided.

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

Audit Recommendation:

The District should regularly review network user accounts and disable those that are unnecessary.

Implementation Plan of Action(s)

Director of Information and Technology will review board agendas to determine new hires as well as determine separations in order to terminate or verify individual's network access.

Implementation Date:

Immediately

Person(s) Responsible for Implementation:

Director of Information and Technology

Audit Recommendation:

Develop an SLA (service level agreement) to address the District's specific needs and expectations for IT services.

Implementation Plan of Action(s)

Penn Yan Central School District will develop a Service Level Agreement that addresses the specific needs and the expectations of the Information Technology Department.

Implementation Date:

By the end of the calendar year (2021).

Person(s) Responsible for Implementation:

Superintendent, Assistant Superintendent for Business, Director of Information Technology

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 interviewed District officials to gain an understanding of IT operations, specifically those related to the granting, modification and revocation of network and local user accounts and permissions.
- We examined network user account and security settings using a specialized audit script. We reviewed the network user and administrator accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts. We reviewed automated settings to identify any settings that indicated ineffective IT controls.
- We followed up with District officials on potentially unneeded accounts and automated settings that indicated ineffective IT controls.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

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

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://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
https://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
https://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
https://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, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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