DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-162

Arkport Central School District

Network Access Controls

JANUARY 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Arkport Central School District

Audit Objective

Determine whether Arkport 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.

- District officials did not establish written policies or procedures to add or disable user accounts and permissions.
- The District had 92 unneeded network user accounts and nine user accounts with unnecessary administrative permissions.

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

Key Recommendations

- Establish written policies or procedures for managing network user accounts.
- Regularly review network user accounts and disable those that are unnecessary.
- 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.

District officials generally agreed with our recommendations and indicated they will take corrective action. Appendix B includes our comment on the District's response.

Background

The District serves the Towns of Almond, Birdsall and Burns in Allegany County, Dansville, Fremont and Hornellsville in Steuben County and a portion of the City of Hornell.

The District is governed by a five-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. He also manages the District's information technology (IT) operations with assistance from Erie 1 Board of Cooperative Educational Services (BOCES) staff who provided both onsite and remote IT services such as technology integration and network administration.

Quick Facts

Enabled Network User Accounts	
Student	489
Non-Student	259
Total	748
IT Vendor Contract Services	
2021 Expenditures	$602,824

Audit Period

July 1, 2020 – September 21, 2021

Network Access Controls

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

Officials should disable unnecessary user accounts as soon as there is no longer a need for them.

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 and processes with access to network resources[1] and should be actively managed to minimize the 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 PPSI, make changes to the records or deny access to electronic information.

A school district should have written procedures for granting, changing, and disabling network user access and permissions. 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. Officials should disable unnecessary user accounts as soon as there is no longer a need for them.

Generic accounts are not linked to individual users and may be needed for certain network services to run properly. For example, generic accounts can be created and used for classroom instructional purposes or to scan student tests. Officials should routinely evaluate generic network user accounts and disable those that are not related to a system need.

Shared network user accounts are accounts with a username and password that are shared among two or more users. Shared accounts are often used to provide network 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).

[1] Network resources include shared folders, centralized printing, email and Internet access.

Because shared accounts are not assigned to a specific user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, each user should have their own user account. In addition, shared accounts should be limited to those instances when multiple users must access one computer to perform assigned duties or temporary work, guests, and have an expiration date.

Generally, a network 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 may inherently run with the same permissions. For example, if malicious software installed itself on a computer, it could 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.

Officials Did Not Establish Policies and Procedures to Manage Network User Accounts and Permissions

District officials did not establish policies or procedures to add or disable user accounts or change user permissions. District officials configured specialized software to automatically manage user accounts on the network.

We examined all 748 enabled network user accounts (489 student accounts, 177 non-student and 82 generic accounts accounts) to determine whether accounts were necessary and appropriate.

Unneeded Network User Accounts – We found 188 inactive user accounts (133 student accounts and 55 non-student accounts) that had not been used in at least six months. District officials reviewed these accounts upon our request and disabled 52 of the 188 accounts (28 percent) and an additional four active user accounts because they were former students and staff. The Superintendent determined the remaining 136 inactive user accounts were needed.

Unneeded Generic and Shared Network User Accounts – Of the 53 shared and 29 generic network user accounts, we found 35 shared and 21 generic user accounts were not used in the last six months. District officials reviewed these accounts and told us they disabled 24 unnecessary shared user accounts and 12 generic user account because they were no longer needed.

In total, officials disabled 92 (12 percent) of the 748 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. 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.

Unnecessary Administrative Permissions – We found 25 accounts with administrative permissions. District officials reviewed these accounts and determined that administrative permissions were unneeded on nine accounts.

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.

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

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt policies and procedures for managing network user accounts, including adding and disabling user accounts and changing user permissions.

District officials should:

2. Regularly review and update network user accounts for necessity and appropriateness and disable those that are no longer needed.
3. 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

ARKPORT
CENTRAL SCHOOL

January 10, 2022

Office of the New York State Comptroller
Edward V. Grant Jr., Chief Examiner
The Powers Building, 16 West Main Street – Suite 522
Rochester, New York 14614-1608

Dear Mr. Grant Jr.,

Please accept this letter as Arkport Central School District's official audit response for audit 2021M-162. The audit, referenced above, covered network access controls for the period of July 1, 2021, to September 21, 2021. The district agrees with the following recommendations made by the audit:

1. "The Board and District officials should develop and adopt written payroll policies for managing network and user accounts, including adding and disabling user accounts and changing user permissions."
2. "Regularly review and update network user accounts for necessity and appropriateness and disable those that are no longer needed."
3. "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."

While the district agrees with the audit's recommendations, the district does not agree, in full, with the following key findings of the audit:

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

The district understands that New York State audits cannot be overly broad in their scope, as this would make the audits difficult to complete. However, the district's audit fails to mention any of the measures in place to protect network access. The Comptroller's office uses the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) as the measure of how a public organization is managing and keeping data private. Within the category of access control, there are multiple subcategories that are not mentioned in the audit report. For instance, the use of multi-factor authentication implemented by the district is not mentioned. If the district will be held to the standard of the NIST CSF, all subcategory components should be mentioned in the final audit report.

See
Note 1
Page 7

ARKPORT
CENTRAL SCHOOL

The Arkport Central School District agrees with recommendations for improvement of network access controls and has already implemented many of the suggested improvements. The district's CAP will outline all changes in policies and procedures that have been and will be implemented. The district plans to approve the CAP at the February regular BOE meeting.

On behalf of the Arkport Central School District,

Jesse Harper
Superintendent of Schools

Appendix B: OSC Comment on the District's Response

Note 1

As part of our audit process we identified to you that we would be using the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) as criteria. NIST CSF is based on existing standards, guidelines and practices and is acceptable criteria for our audit. The results using this criteria provide the District with a performance measurement tool and a means to reduce cybersecurity risk.

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

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 and procedures and interviewed District and BOCES officials to gain an understanding of IT operations, specifically those related to granting, modifying and revoking network user accounts and permissions.
- We examined network user account and security settings using a computerized audit script run on July 20, 2021. We reviewed the network user accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts and permissions. We reviewed automated settings to identify any settings that indicated ineffective network access controls.
- We identified inactive network user accounts and followed up with District officials on potentially unneeded accounts and automated settings that indicated ineffective network access 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 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, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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