REPORT OF EXAMINATION | 2021M-30

New Lebanon Central School District

Network User Accounts

JUNE 2021

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

Contents

Report Highlights

New Lebanon Central School District

Audit Objective

Determine whether New Lebanon Central School District (District) officials established adequate internal controls over network user accounts to prevent unauthorized use, access and loss.

Key Findings

Officials did not establish adequate controls over the District's network user accounts to protect against unauthorized use, access and loss. Officials did not:

- Disable 26 unneeded generic accounts of the 48 generic network accounts examined.
- Ensure acceptable use policy (AUP) compliance.
- Monitor the use of the information technology (IT) resources.
- Provide IT security awareness training to all employees using IT resources.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop and implement written procedures for granting, changing and disabling user permissions and monitoring compliance with the AUP.
- Maintain an authorized network user list and routinely evaluate and disable unneeded accounts.

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

Background

The District serves the five towns of New Lebanon, Canaan, Stephentown, Chatham and East Nassau in Columbia County. The District is governed by a Board of Education (Board), which has seven elected members.

The Superintendent of Schools (Superintendent) is appointed by the Board and is the chief executive officer responsible for day-to-day management, under the Board's direction.

District officials and staff rely on the District's IT assets for Internet access, email and maintaining confidential and sensitive financial and personnel records. The District's Network Systems Engineer (Engineer) is responsible for monitoring network user accounts.

Quick Facts	
Network User Accounts[a]	738
Employees	110
Students	436

a) These included 117 employee, 573 student and 48 generic accounts.

Audit Period

July 1, 2019 – September 18, 2020. We extended our scope forward to December 7, 2020 to complete our IT testing.

Network User Accounts

The District's IT system and data are valuable resources. The District relies on its IT assets for Internet access, email and maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI).[1] 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.

...[D]istrict officials should regularly review enabled network user accounts... and disable unnecessary accounts.

How Should District Officials Manage Network User Accounts?

Network user accounts provide access to networks and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. A district should have written procedures for granting, changing and disabling user permissions. In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed. Officials should disable unnecessary 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 or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Officials should routinely evaluate and disable any generic accounts that are not related to a specific system need.

Officials Did Not Adequately Manage Network User Accounts

The Engineer was responsible for ensuring network user accounts were managed in a timely and satisfactory manner. However, network user accounts were inadequately managed. Officials did not maintain a list of authorized network users. As a result, we found 26 unneeded network user accounts that had not been disabled.

Further, the District did not have written procedures for granting, changing and disabling user permissions. Because they did not maintain a current list of authorized users, they were unable to review or monitor user access. The Engineer told us that being a small district there is more a culture of compliance.

1 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.

We reviewed all 48 generic accounts and found 26 generic accounts that were originally created for various uses and were no longer needed. The Engineer told us he was not informed by staff when they no longer needed the accounts and indicated that he will disable the accounts.

If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. Because generic accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user.

How Should Officials Monitor Compliance with the AUP?

A district should have a written AUP that defines the procedures for computer, Internet and email use and describes what constitutes appropriate and inappropriate use of IT resources, management's expectations concerning personal use and consequences for violating the AUP.

District officials should develop procedures for monitoring compliance with a district's AUP. Procedures should include routinely monitoring Internet use and requiring web filtering software to block access to unacceptable websites and limit access to sites that do not comply with a district's AUP.

Officials Did Not Monitor Compliance with the AUP

The District's comprehensive AUP defines the terms for computer, Internet and email use. Also, the policy describes what constitutes appropriate and inappropriate use of IT resources, along with District management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP.

However, officials and direct supervisors did not monitor employee Internet use or implement procedures to monitor for compliance with the AUP. We examined the web browsing history of three computers used by five employees whose job duties routinely involved accessing PPSI to determine whether they were used for nonbusiness purposes.

We found evidence of personal use on four of the five employee network user accounts (Figure 1). The Engineer told us that he relied on the antivirus/web filter agent to log and prevent access to inappropriate sites[2] and was unaware of any questionable Internet use.

2 A web filter is not inherently a monitoring tool on its own; it allows for blocking known prohibited websites and recording logs of visited websites, but those logs would then need to be periodically reviewed for appropriateness.

Figure 1: Examples of Personal Internet Use

Type	Website
Real estate	realtor.com, trulia.com, zillow.com
Entertainment	beargoggleson.com, bearswire.com, bleacherreport.com, nbcsports.com, sportsmonkey.com
Social media/Genealogy	facebook.com, ancestry.com
Shopping	amazon.com, blinkforhome.com, ebay.com, gamestop.com, google.com, lowes.com, walmart.com, hobbylobby.com
Personal email	gmail.com, juno.com, yahoo.com
News media	foxnews.com
Personal online banking	citigroup.com, greylockfederalcreditunion.org

When employees access websites for nonbusiness or inappropriate purposes through the network, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections (malware).

Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training. The training should explain policies and procedures to all employees and communicate the proper rules of behavior for using the Internet and IT systems and data.

The training should center on emerging trends such as information theft, social engineering attacks, computer viruses, and other types of malicious software, all of which may result in PPSI compromise or denying access to the IT system and its data. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

Furthermore, District policy states the Superintendent shall be responsible for providing in-service programs for the training and development of District staff in computer skills and for the incorporation of computer use in appropriate subject areas. The Superintendent shall be responsible for ensuring that staff and students receive training including on computer network use.

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training.

District Officials Did Not Provide IT Security Awareness Training

District officials did not provide all employees with IT security awareness training to help ensure they understand IT security measures designed to safeguard data and IT assets. We selected a sample of three employees who regularly access PPSI and found that all three administrative office staff had not received IT security awareness training.

The Engineer said that staff were provided security awareness training during professional development days. However, administrative office staff did not receive the training. As a result, IT assets and data were more vulnerable to loss and misuse. Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

District officials should:

1. Develop written procedures for granting, changing and disabling user permissions.
2. Design and implement procedures to monitor employee computer use and implement procedures to monitor for compliance with policy.
3. Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use.

The Network Systems Engineer should:

4. Maintain a list of authorized network users and routinely evaluate and disable any unnecessary accounts.
5. Monitor computer Internet use to ensure employees comply with the AUP.

Appendix A: Response From District Officials

New Lebanon
Central School
District

5/13/2021

Dear Ms. Lisa Reynolds,

I write in response to the draft audit report on the "New Lebanon Central School District - School District IT Audit" (Audit number - 2021M-30-IT.) After reviewing this report I agree with its findings. The recommendations will ensure that our IT systems have no vulnerabilities that significantly increase the probability of a disruption or compromise or our data systems.

As the new superintendent of the New Lebanon Central School District, I am using this audit as an opportunity to enhance our IT procedures and security. I have already met with stakeholders and made plans to develop a more detailed IT procedure and protocol handbook. Our systems manager has already made several updates and changes to our systems as recommended by the audit with the goal of securing our IT systems. Once the corrective action plan is complete, the plan will be posted on our website under our audit section.

Please let me know if you have any other questions or need any additional information from the district. I look forward to seeing the final audit report.

Sincerely,

Andrew Kourt
New Lebanon CSD Superintendent

14665 State Route 22
New Lebanon,
New York
12125

phone: 518.794.9016
fax: 518.766.5574

www.newlebanoncsd.org

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 the District's network user accounts and determine the adequacy of the policies and procedures.
- We inquired with District officials regarding whether they received IT security awareness training and how they are notified of policy changes and updates to the IT policy.
- We ran a computerized audit script to examine the District's domain controller. We then analyzed the report by comparing user accounts to a list of current employees to determine whether any network users were no longer employed by the District.
- We examined the web browsing histories on three computers to determine whether Internet use was in compliance with the District's AUP. We used our professional judgment to select five employee network user accounts based on job duties that involve accessing PPSI.

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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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