



Edgemont Union Free School District

Information Technology

2024M-37 | November 2024

Contents

Report Highlights 1

Nonstudent Network User Accounts 2

 How Should Officials Manage Nonstudent Network User Accounts? 2

 The IT Director Did Not Adequately Manage Nonstudent Network User Accounts 2

 What Do We Recommend? 3

Appendix A – Response From District Officials 4

Appendix B – Audit Methodology and Standards 5

Appendix C – Resources and Services. 6

Report Highlights

Edgemont Union Free School District

Audit Objective

Determine whether Edgemont Union Free School District (District) officials disabled unnecessary user accounts in a timely manner.

Key Findings

The IT Director did not disable unnecessary user accounts in a timely manner. As a result, the District had an increased risk of unauthorized access to and use of the network and could potentially lose important data. In addition to sensitive information technology (IT) control weaknesses that we communicated confidentially to officials, we reviewed all 665 nonstudent network user accounts and determined that District officials did not:

- Disable 34 unneeded network user accounts that had users with separation dates ranging from July 12, 2021 to July 1, 2023. The accounts included:
 - 14 former employee accounts,
 - 12 consultant accounts, and
 - Eight service accounts.
- Develop written procedures for adding, modifying or disabling nonstudent network user accounts.

Key Recommendations

- Ensure that written procedures for disabling network user account access are implemented and followed.
- Maintain a list of authorized user accounts and routinely evaluate and disable any unneeded network user accounts in a timely manner.

District officials generally agreed with our findings and recommendations and indicated they will initiate corrective action.

Audit Period

July 1, 2022 – July 20, 2023

Background

The District is located in the Town of Greenburgh in Westchester County.

The Board of Education (Board) is composed of seven elected members and is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District contracts with the Lower Hudson Regional Information Center (LHRIC) to help manage the District's day-to-day IT operations. LHRIC staff report directly to the District's Director of Technology and Information Systems (IT Director). The IT department is composed of District and LHRIC technicians.

Quick Facts

Nonstudent Network User Accounts

Employee	491
Service	108
Other	66
Total	665

Nonstudent Network User Accounts

How Should Officials Manage Nonstudent Network User Accounts?

Nonstudent network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access and loss. Nonstudent network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view personal, private and sensitive information (PPSI)¹ on the network, make unauthorized changes to official school district (district) records or deny legitimate access to network resources.

To actively manage network user accounts, when network user accounts are no longer needed, they should be disabled in a timely manner. Additionally, district officials should maintain a list of authorized network user accounts and routinely review enabled network user accounts to ensure they are still needed and disable unneeded network user accounts.

District officials should develop and implement written procedures for periodically reviewing enabled user accounts to ensure they are still needed and disabling nonstudent network user accounts as soon as they are no longer needed. These procedures should be distributed to all applicable district and vendor staff to be used in carrying out their assigned duties related to network user account management.

The IT Director Did Not Adequately Manage Nonstudent Network User Accounts

The IT Director did not adequately manage nonstudent network user accounts. The IT Director did not establish written procedures for disabling nonstudent network user accounts. Instead, he relied on LHRIC technicians to help manage the District's network user accounts. However, the IT Director was responsible for overseeing the work of LHRIC technicians. In addition, LHRIC technicians would not know when a user account needs to be disabled without receiving notification from District officials to disable the accounts.

The District implemented automated procedures for disabling employee network user accounts on March 20, 2023. When an employee was disabled in the payroll system, their network user account was also automatically disabled. However, these procedures only applied to employees who separated from the District after March 20, 2023, and did not include service or other network user accounts, such as those belonging to Board members and contractors. LHRIC technicians were responsible for managing all service network user accounts based on instructions from the IT Director.

We reviewed all 665 nonstudent network user accounts and identified 34 user accounts that were unneeded and should have been disabled, including 14 former employee accounts, 12 former contractor accounts² and eight service accounts.³ The users of these unneeded accounts had separation dates ranging from July 12, 2021 to July 1, 2023. The IT Director stated that they conduct an audit of network user accounts, which includes reviewing all authorized users and their access, each

¹ PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, students, employees, third parties or other individuals or entities.

² These accounts included third-party users, such as digital arts consultants, outsourced cafeteria staff and a construction supervisor.

³ Service accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, service accounts can be created and used for automated backups.

summer. In addition, contractor network accounts are audited at least twice a year by the Technology and Business departments and Board members are audited after each Board of Education election. Therefore, these accounts were set to be removed when they performed their regular summer network account audit. However, if the reviews had been performed, at least 12 of the unneeded accounts would have been identified and disabled prior to our audit. The IT Director also stated that disabling an account does not require a written procedure because the process is part of the everyday workflow. However, without written procedures, the IT department did not have a process to periodically review active network accounts or determine when the nonstudent and nonemployee user accounts were no longer needed and should be disabled.

After the audit team discussed these findings with the IT Director, he established review procedures for disabling nonstudent and nonemployee network user accounts, including the use of a nonemployee account approval form. A copy of these procedures, including the form, was provided to the audit team. We reviewed these procedures and determined that they appeared reasonable.

If not adequately managed, unneeded nonstudent network user accounts may not be detected and disabled in a timely manner. When unneeded nonstudent network user accounts remain enabled, they are potential entry points for attackers because, if compromised, they could be used to inappropriately access the network and view any PPSI accessible through that account's access, make unauthorized changes to District records, deny legitimate access to electronic information, or gain access to or control over other IT functions.

What Do We Recommend?

The IT Director should:

1. Develop written procedures for disabling nonstudent network user accounts, distribute the procedures to applicable staff, and ensure that employees and LHRIC technicians implement and comply with the procedures.
2. Ensure a list of authorized user accounts is maintained and routinely reviewed and evaluated, and unneeded nonstudent network user accounts are disabled in a timely manner.

Appendix A: Response From District Officials



EDGEMONT UNION FREE SCHOOL DISTRICT

Central Office

300 White Oak Lane · Scarsdale, New York 10583
Dr. Kenneth R. Hamilton, Superintendent of Schools

August 20, 2024

Dara Disko-McCagg
Chief Examiner
Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 102
New Windsor, NY 12553

Sent Via Email to: Muni-Newburgh@osc.ny.gov

Dear Ms. Disko-McCagg:

The Edgemont Union Free School District is in receipt of the draft Report of Examination 2024M-37, covering the period from July 1, 2022 through July 20, 2023. This audit aimed to determine whether Edgemont Union Free School District officials disabled unnecessary user accounts in a timely manner. The District has reviewed the New York State Comptroller's Audit Report. We thank the Office of the State Comptroller for conducting a comprehensive audit of our non-student network accounts. Additionally, we thank the local field staff who conducted this most recent audit. They were professional and courteous throughout their time here in Edgemont.

The Edgemont School District always welcomes feedback as we strive for continued improvements and has made tremendous strides in Information Technology management over the past decade. Your feedback and recommendations serve as a tool to assist the District in furthering this endeavor.

While the findings of the report are not disputed by the District, we do wish to provide the following additional details. Reliance on technology in The Edgemont Union Free School District has grown exponentially in recent years. To that end, the implementation of new systems, infrastructure, devices, and networks is constantly evolving. This audit highlighted opportunities to improve our systems managed by The Lower Hudson Regional Information Center (LHRIC) and work with our new Human Resources Department as an additional resource in strengthening the management and safety of our staff network access.

Our technology department continuously reviews and internally audits our practices and policies to ensure we follow industry standards and best practices. However, we remain receptive to outside feedback and proposed means to improve our systems further. To that end, the District views the OSC findings as easily rectified to protect our technology systems further.

On behalf of the Edgemont Union Free School District, I thank the OSC for keeping all New York school districts secure and accountable.

Sincerely,

Dr. Kenneth R. Hamilton
Superintendent of Schools

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. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We reviewed the District's IT policies and procedures and interviewed the IT Director, Assistant Superintendent for Business and LHRIC technicians to gain an understanding of the District's IT environment and internal controls related to network user account management, and to determine whether the policies and procedures were adequate.
- We ran a computerized audit script on July 20, 2023 to examine the District's domain controller. The District had a total of 2,540 enabled network user accounts. We excluded the 1,875 student accounts and examined the 655 nonstudent network user accounts.
- We compared the enabled nonstudent network user accounts to a list of current employees and interviewed the IT Director and Assistant Superintendent for Business regarding unused and other potentially unneeded accounts to identify accounts that are no longer needed.
- We inquired about the District's procedures for disabling nonstudent network user accounts and reviewed the District's procedures for disabling employee network user accounts to gain an understanding of their process for disabling nonstudent network user accounts.

Our audit also examined the adequacy of certain IT 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 school 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.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas

www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems

www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders

www.osc.ny.gov/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.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers

www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics

www.osc.ny.gov/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

<https://www.osc.ny.gov/local-government>

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief of Municipal Audits

33 Airport Center Drive, Suite 102 • New Windsor, New York 12553-4725

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

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties