DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-18

Ellenville Central School District

Network User Accounts

JUNE 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Ellenville Central School District

Audit Objective

Determine whether Ellenville Central School District (District) officials ensured network user accounts were adequately managed.

Key Findings

District officials did not ensure network user accounts were adequately managed. In addition to sensitive information technology (IT) control weaknesses which we communicated confidentially to officials, we found District officials should have:

- Disabled 550 network user accounts that were no longer needed. Of the 550 unneeded accounts, 462 were not used to log into the District's IT system in at least six months from the date of our test.
- Established written procedures for granting, changing or disabling network user accounts.

Key Recommendations

- Develop written procedures for granting, changing and disabling user access.
- Maintain a list of authorized user accounts and routinely evaluate and disable any unnecessary user accounts.

District officials agreed with our recommendations and indicated they will take corrective action.

Background

The District is located in the Towns of Wawarsing and Rochester in Ulster County and the Town of Mamakating in Sullivan County. The District is governed by a Board of Education (Board), which comprises nine elected Board Members. The Board is responsible for the general administration of the District through setting policies and expectations.

The Superintendent of Schools (Superintendent) is appointed by the Board and is responsible for day-to-day management.

The District's Director of Technology (Director) is the head of the IT department and is responsible for managing network user accounts.

Quick Facts	
Students	1,555
Employees	400
Network User Accounts	
Student	1,926
Employee	406
Generic	402
Non-employee	90
Total	2,824

Audit Period

July 1, 2019 – March 31, 2021. We extended the audit scope through July 13, 2021 to complete our IT testing.

Network User Accounts

How Should District Officials Manage Network User Accounts?

Network user accounts provide access to network resources 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 personal, private and sensitive information (PPSI)[1] on the network or to gain access to or control over other IT functions. Therefore, a district should have written procedures for granting, changing and disabling user accounts.

Officials should disable unnecessary accounts as soon as there is no longer a need for them. In addition, to minimize the risk of unauthorized access, district officials should maintain a list of authorized user accounts and 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. Therefore, they should be limited in use as they have reduced accountability. 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 generic network user accounts and disable those that are not related to a specific district or system need.

District Officials Did Not Adequately Manage Network User Accounts

The Director was responsible for ensuring network user accounts were managed in a timely and satisfactory manner. However, he did not adequately manage the District's network user accounts. The Director did not maintain a list of authorized network user accounts or periodically review active accounts to confirm they were needed and properly authorized.

We reviewed all 2,824 enabled network user accounts and identified 550 unneeded network user accounts that had not been disabled. These accounts included:

- 252 generic accounts, of which 191 had not been used in at least six months,
- 216 former student accounts which had not been used in at least six months,
- 79 nonemployee[2] accounts, of which 52 had not been used in at least six months, and

[1] Personal, private or sensitive information (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.

[2] Nonemployee accounts would include those of Board members, former employees and third-party contractors.

- Three substitute teachers' accounts which had not been used in at least six months.

District officials did not develop written procedures for granting, changing and disabling user accounts. Although a list of all enabled user accounts was available, the Director did not review the list to confirm active network user accounts were properly approved and needed. If the Director properly reviewed the network user accounts, the unneeded accounts would have been identified.

Both the Assistant Superintendent for Business and the Director stated that when a new Director comes on, there is an assumption that the previous directors were diligent in their duties. In addition, they stated the current Director had a small staff and when the pandemic hit the expansion of the IT Department was needed to manage remote learning. However, the audit's aggregate findings indicate current officials must exercise more diligence to ensure the District's network is sufficiently safeguarded from unauthorized access. Furthermore, cybersecurity risks should be treated as any other hazard a school district may encounter. The potential risks could have a significant impact on the District's IT operations. As such, the District should have obtained and/or allocated resources to ensure the risks associated with unneeded accounts were addressed timely.

When we brought our findings to the attention of District officials, the Director reviewed all network user accounts and began addressing the issues immediately. However, the Director should establish and follow a process, preferably automated, to reduce the risk of human error, to the extent possible, for disabling accounts immediately upon termination or role change of a user. In addition, he should periodically generate and review a list of users from the system and verify whether all users are active and disable those that are no longer needed.

When network user accounts are not used or monitored, compromised accounts may not be detected timely. Without written procedures, employees may not be aware of their responsibilities when students and staff leave the District.

What Do We Recommend?

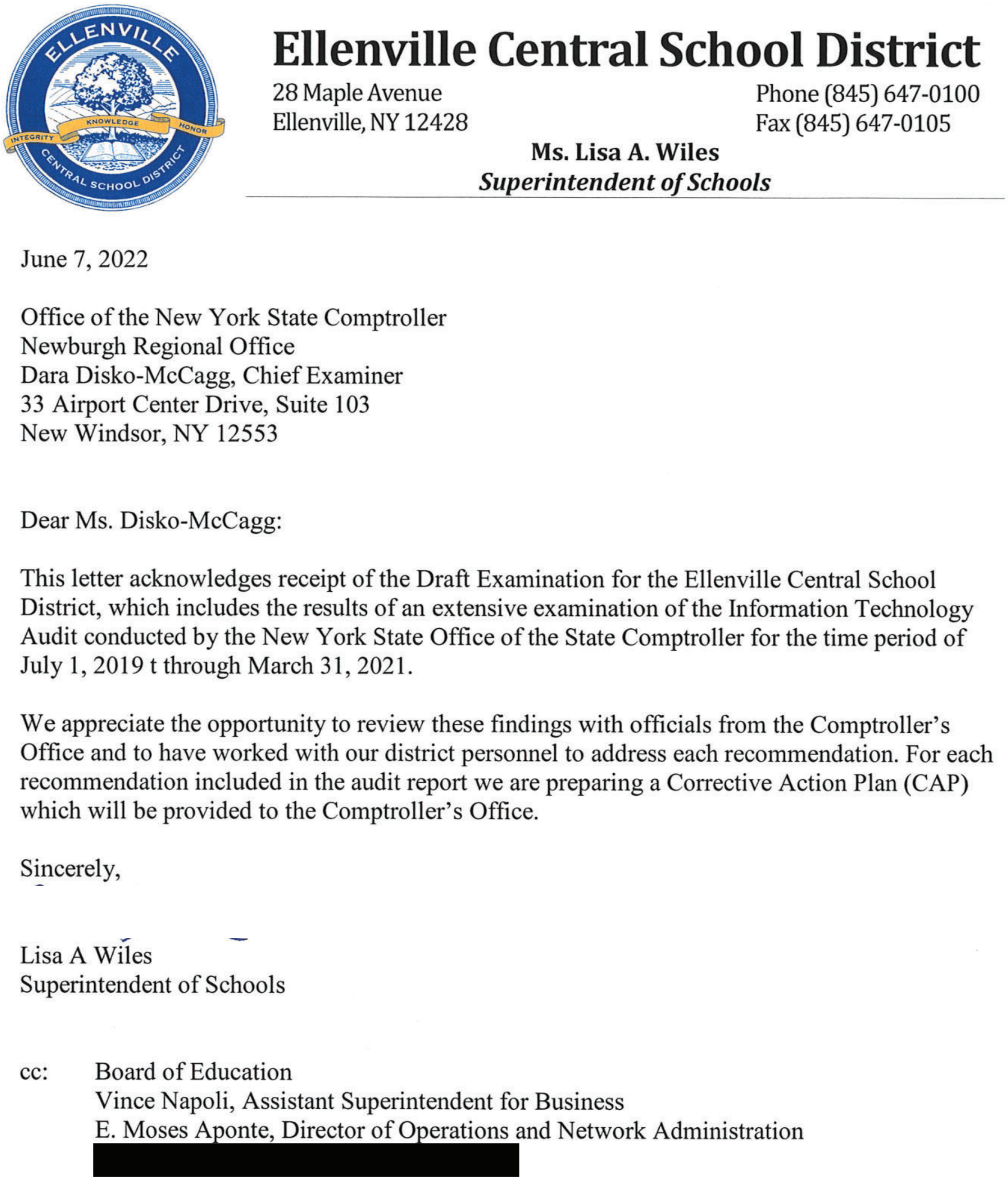
District officials should:

1. Develop written procedures for granting, changing and disabling network user accounts and ensure such procedures are implemented and adhered to.

The Director should:

2. Maintain a list of authorized user accounts and routinely evaluate and disable any unnecessary network user accounts.

Appendix A: Response From District Officials



Ellenville Central School District

28 Maple Avenue
Ellenville, NY 12428

Phone (845) 647-0100
Fax (845) 647-0105

Ms. Lisa A. Wiles
Superintendent of Schools

June 7, 2022

Office of the New York State Comptroller
Newburgh Regional Office
Dara Disko-McCagg, Chief Examiner
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

Dear Ms. Disko-McCagg:

This letter acknowledges receipt of the Draft Examination for the Ellenville Central School District, which includes the results of an extensive examination of the Information Technology Audit conducted by the New York State Office of the State Comptroller for the time period of July 1, 2019 t through March 31, 2021.

We appreciate the opportunity to review these findings with officials from the Comptroller's Office and to have worked with our district personnel to address each recommendation. For each recommendation included in the audit report we are preparing a Corrective Action Plan (CAP) which will be provided to the Comptroller's Office.

Sincerely,

Lisa A Wiles
Superintendent of Schools

cc: Board of Education
Vince Napoli, Assistant Superintendent for Business
E. Moses Aponte, Director of Operations and Network Administration
[redacted]

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 how the District manages its network user accounts and determine the adequacy of those policies and procedures.
- We interviewed District officials and reviewed records to gain an understanding of procedures related to managing, configuring and securing network user accounts.
- We ran a computerized audit script to examine the District domain controller.[3] We then analyzed each report generated by the script, looking for weaknesses in network user account management, privilege and group definition and network setting configurations. We also compared the list of network user accounts generated by the script to a list of current employees to determine whether any network users were no longer employed by the District. We discussed with District officials any potentially unnecessary network user accounts and any network security settings that did not meet industry best practices.

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.

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.

[3] The server that controls or manages access to network resources.

Appendix C: 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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, 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: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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