REPORT OF EXAMINATION | 2021M-145

Highland Falls-Fort Montgomery Central School District

Network User Accounts

JUNE 2022

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

Contents

Report Highlights

Highland Falls-Fort Montgomery Central School District

Audit Objective

Determine whether Highland Falls-Fort Montgomery Central School District (District) officials adequately managed and secured network user accounts.

Key Findings

The Technology Department could improve how they manage and secure network user accounts. Specifically:

- They did not establish comprehensive written procedures for managing network user accounts.
- Forty-eight network user accounts, including 22 non-student accounts, 16 generic accounts, and 10 student accounts, were unneeded and should have been disabled.

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

Key Recommendations

- Establish comprehensive written procedures for managing network user accounts.
- Regularly review enabled network user accounts and ensure that unneeded user accounts are immediately disabled.

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

Background

The District is located in the Town of Highlands in Orange County.

The District is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent is the District's 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 Assistant Superintendent for Curriculum, Instruction and Technology (Assistant Superintendent) oversees the Technology Department that is responsible for managing and securing network user accounts.

Quick Facts

Network User Accounts	
Student	945
Non-Student	298
Generic	40
Total	1,283
Reviewed	1,283

Audit Period

July 1, 2019 – April 20, 2021

Network User Accounts

The District's IT system and data are valuable resources. The District relies on its IT assets for maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI)[1] and is accessed through network user accounts, email and Internet access. 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, such as adequately managed and secured network user accounts, will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

If not adequately managed and secured, network user accounts could be potential entry points for attackers. …

How Should Officials Adequately Manage and Secure Network User Accounts?

Network user accounts provide access to network resources such as shared folders and email, and should be properly managed and secured to minimize the risk of misuse. If not adequately managed and secured, network user accounts could be potential entry points for attackers, because they could be used to inappropriately access and view PPSI on the network. In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed. A district should also have comprehensive written procedures for managing network user accounts, including granting user permissions based on the users' responsibilities, changing and disabling user permissions. Officials should disable unnecessary accounts as soon as they are no longer needed.

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. IT managers should limit use of generic network user accounts, because they may not be able to trace user activity to a single user for these accounts. Officials should routinely evaluate generic network user accounts and disable those that are not related to a current district or system need.

District Officials Could Improve How They Manage and Secure Network User Accounts

District officials could improve how they manage and secure network user accounts. We reviewed all 1,283 network user accounts to identify inactive user accounts and determine whether they were needed. Next, we discussed with

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 (students), third parties or other individuals or entities.

the former Assistant Superintendent the need for 470 network user accounts (37 percent) that had not been used in more than six months (composed of 343 student, 99 non-student and 28 generic accounts). Based on this discussion and further review, we identified 48 accounts that were not needed. Specifically, we found:

- 22 non-student accounts, of which, 18 were assigned to former employees. For example, a former teacher's aide had an enabled network user account for more than one year after separation. The remaining four unneeded users included former Board members, a duplicate Board member user account, and a former intern.
- 16 generic accounts mostly used as backup or testing accounts, and some had elevated permissions to the District's network.
- 10 student accounts were assigned to former students that are no longer at the District, including four accounts that were never used.

The former Assistant Superintendent told us that these accounts were not necessary and should have been disabled. However, she could not provide us with a reason why the accounts were not disabled. The Technology Department developed informal procedures for maintaining and periodically reviewing a current list of authorized users and their levels of access. However, we found that these procedures were not always followed.

Stale and unneeded network user accounts are additional entry points into a network and, if accessed by an attacker or a former employee, could be used to inappropriately access and view PPSI. Because some of the unneeded user accounts were for former teachers, sensitive student information could have been inappropriately accessed, modified or deleted if these accounts were compromised. These inactive and unneeded accounts may also consume certain network resources which could be allocated elsewhere. When network user accounts are not used or monitored, compromised accounts may not be detected in a timely manner..

What Do We Recommend?

The Technology Department should:

1. Establish comprehensive written procedures for managing network user accounts.
2. Ensure that enabled network user accounts are regularly reviewed and unneeded user accounts are immediately disabled.

Appendix A: Response From District Officials

HIGHLAND FALLS-FORT MONTGOMERY
CENTRAL SCHOOL DISTRICT

Mr. Michael McElduff, Acting Superintendent

May 12, 2022

Dear [redacted]

Thank you again for taking the time to meet in regards to the audit on Friday, May 6, 2022. Please accept this letter as the District's acknowledgement that we received the recommendations from your office and will put together a corrective action plan. Prior to our submission of the corrective action plan, it will be approved by the Board of Education.

Thank you,

Superintendent's Office
845-446-9575

www.hlfmcsd.org
P.O. Box 287, Highland Falls, NY 10928

Fax
845-446-3321

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 the former Assistant Superintendent and District IT staff to gain an understanding of how District officials managed and secured network user accounts and determine the adequacy of the policies and procedures related to network user account management and security.
- We ran a computerized audit script on April 20, 2021 to examine the District's network user accounts and their password and account settings.
- We reviewed the network user accounts' last logon dates to identify inactive and possibly unneeded network user accounts. We compared the password and account settings to industry standards. We then followed up with the former Assistant Superintendent and Technology Department staff on inactive and possibly unneeded network user accounts, and settings that were inconsistent with industry standards.

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 to District's website for public review.

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