



Hastings-on-Hudson Union Free School District

Information Technology

2023M-104 | December 2023

Contents

- Report Highlights 1**

- Network User Accounts 2**
 - How Should District Officials Ensure That Unneeded Network User Accounts Are Disabled in a Timely Manner? 2

 - District Officials Did Not Ensure That Unneeded Network User Accounts Were Disabled. 2

 - What Do We Recommend? 4

- Appendix A – Response From District Officials 5**

- Appendix B – Audit Methodology and Standards 6**

- Appendix C – Resources and Services. 8**

Report Highlights

Hastings-on-Hudson Union Free School District

Audit Objective

Determine whether Hastings-on-Hudson Union Free School District (District) officials ensured that unneeded network user accounts were disabled in a timely manner.

Key Findings

District officials did not ensure that unneeded network user accounts were disabled in a timely manner. As a result, 21 percent of the District's network user accounts were unneeded and additional entry points that could have been used to inappropriately access the network and view personal, private and sensitive information (PPSI), make unauthorized changes to records, deny legitimate access to electronic information, or gain access to or control over other information technology (IT) functions.

In addition to sensitive IT control weaknesses we communicated confidentially to District officials, we found that officials did not:

- Convey management's expectations for managing network user accounts through written policies and procedures.
- Disable 551 unneeded network user accounts. These accounts had last log on dates ranging from March 2014 to November 2022.

Key Recommendations

- Convey management's expectations for managing network user accounts through written policies and procedures.
- Routinely evaluate network user accounts for necessity, disable any unneeded accounts and monitor staff to ensure unneeded accounts are disabled in a timely manner.

District officials agreed with our findings and recommendations and indicated they plan to initiate corrective action.

Background

The District is located in Westchester County and governed by an elected seven-member Board of Education (Board) responsible for managing and controlling the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is the chief executive officer appointed by the Board and is responsible for ensuring IT policies, guidelines and procedures are implemented effectively.

The District contracted with the Lower Hudson Regional Information Center (LHRIC) to provide managed IT and field support services. The Business Official is responsible for overseeing the District's IT operations, including the management of network user accounts

Quick Facts

Network User Accounts

Type	Enabled	Unneeded
Student	2,043	397
Employee	368	17
Other	252	137
Total	2,663	551

Audit Period

July 1, 2021 – September 15, 2022. We extended our scope forward to November 4, 2022, to complete our IT testing.

Network User Accounts

Network user accounts provide access to network resources and as such are potential entry points for attackers to gain unauthorized access to, use or cause the loss of those resources. If not adequately managed, network user accounts could be used to inappropriately access the network and view PPSI,¹ make unauthorized changes to records, deny legitimate access to electronic information, or gain access to or control over other IT functions.

How Should District Officials Ensure That Unneeded Network User Accounts Are Disabled in a Timely Manner?

School district (district) officials should ensure unneeded network user accounts are disabled in a timely manner by developing and enforcing written procedures for disabling user accounts. These procedures should be distributed to all applicable staff to be used in carrying out their assigned duties related to network user account management. District officials should monitor staff to ensure they are in compliance with the procedures.

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 if the assigned rights are appropriate for an employee's duties. Officials should disable unneeded network user accounts and adjust access rights, when necessary.

District Officials Did Not Ensure That Unneeded Network User Accounts Were Disabled

The Superintendent and Business Official did not establish written procedures for managing unneeded network user accounts and did not maintain a list of enabled network user accounts or review the accounts to identify and remove unnecessary accounts. District officials said they relied on LHRIC to perform these duties. However, LHRIC consultants stated that the District did not request this service and they do not provide additional services unless requested by the District. Because the District no longer had an IT Director and the Business Official was responsible for overseeing IT operations, District officials were not aware of the need to ask LHRIC to perform these services and to ensure they were being performed.

Employee and Student User Accounts – We reviewed all 368 enabled employee network user accounts and identified 17 accounts that were unneeded and should have been disabled. The users of these unneeded accounts included:

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, students, third parties or other individuals or entities.

-
- Eight employees who resigned,
 - Five terminated employees,
 - Three retired employees, and
 - One contracted employee that the District replaced.

The 17 employees separated from District service between June 2019 and October 2022. The Clerk stated that she managed network user accounts and some accounts were not disabled during the period she managed the accounts due to an oversight on her part.

We also reviewed all 2,043 enabled student network user accounts and determined that 397 accounts were unneeded and should have been disabled. These unneeded student accounts included:

- 374 accounts assigned to unenrolled students,
- 13 duplicate accounts,
- Seven accounts that the Registrar could not match to known students, and
- Three accounts for students who graduated in June 2022.

The 374 students left enrollment from the District between March 2014 and November 2022. In addition, 251 unneeded student accounts (63 percent) out of the 397 accounts were never used to log into the network. Although the unneeded active network accounts were not used to access the District's system, the accounts were unneeded entry points that should have been disabled to reduce the risk of unauthorized access.

The Registrar, who started with the District in September 2022, stated that she submitted a service ticket to LHRIC to disable student network user accounts. However, we reviewed a sample of 10 of the 397 unneeded student network user accounts to determine whether a service ticket was submitted to disable the accounts. We determined that all 10 service tickets were not submitted by the current Registrar prior to our inquiry of the unneeded accounts but were submitted three weeks after our inquiry. District officials could not explain why the student user accounts were not disabled in a timely manner.

Other User Accounts – We reviewed all 2,663 network user accounts and determined that 252 accounts were not employee or student accounts. These other user accounts included 191 service accounts,² 36 LHRIC accounts and 25 miscellaneous accounts. We determined that 137 of the other network user accounts were unneeded and should have been disabled, including:

² A service account is created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems).

-
- 133 service accounts,
 - Three LHRIC accounts, and
 - One contractor account.

The Business Official stated that the 137 unneeded network user accounts were not disabled because the District did not inform LHRIC to disable these other accounts because they were not aware the accounts were potential entry points into the network.

When not adequately managed, unnecessary network user accounts may not be detected and disabled in a timely manner. Unnecessary network user accounts are additional entry points into a network and, if accessed by an attacker, could be used to inappropriately view financial, personnel and student records, much of which contain PPSI.

Unnecessary
network user
accounts are
additional
entry points
into a
network. ...

What Do We Recommend?

District officials should:

1. Convey management's expectations for managing network user accounts through written policies and procedures.
2. Routinely evaluate network user accounts for necessity, disable any unneeded accounts and monitor staff to ensure unneeded accounts are disabled in a timely manner.

Appendix A: Response From District Officials



Hastings-on-Hudson Public Schools

Office of the Superintendent
27 Farragut Avenue, Hastings-on-Hudson, New York 10706
tel: (914) 478-6205 fax: (914) 478-6209
www.hohschools.org



William S. McKersie, Ph.D.
Superintendent of Schools
mckersiew@hohschools.org

November 29, 2023

Ms. Dara Disko-McCagg, Chief of Municipal Audits
Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Dear Ms. Disko-McCagg,

We have closely reviewed the Information Technology Audit from the Office of the State Comptroller. The insights provided in the audit are valuable. On behalf of the Board of Education and the District's administrative team, we thank the State Comptroller's Office for their efforts and professionalism.

In reviewing the report with our internal team, we agree with the findings and recommendations, and we are actively working to address them. The District contracts with our local BOCES LHRIC to provide oversight of our Technology Department. Our IT department is collaborating with our technology consultants to ensure that all issues are resolved properly and promptly.

In response to the audit, the District has taken or is in the process of taking the following actions:

- Disabling all unnecessary network accounts
- Creating a process for routinely evaluating user accounts.
- Developing comprehensive written board policies and regulations for technology.
- Developing procedures to be shared with BOCES for managing network user accounts.

We appreciate the time and effort invested in this audit. Thank you again for your valuable contributions to our efficiency and effectiveness.

Sincerely,

William S. McKersie, Ph.D.
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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies, procedures and contract with LHRIC and interviewed District officials and LHRIC staff to gain an understanding of the District's IT environment and how District officials managed network user accounts. We also determined whether the policies, procedures, and contract were adequate.
- We ran a computerized audit script on the District's network on November 4, 2022. We analyzed the reports generated by the script and reviewed all enabled network user accounts. We compared the enabled employee network user accounts to a list of current employees to identify accounts that were assigned to former employees. We compared the enabled student network user accounts to a list of enrolled students to identify student accounts which were no longer needed. We compiled a list of other network user accounts identified by the script as not being used to log into the network prior to May 2022 and within six months of the audit script date and provided the list to LHRIC staff to determine whether there were potentially unneeded other network user accounts.
- We followed up with the Business Official, Deputy Treasurer, Registrar, Clerk and LHRIC staff to determine why unneeded accounts remained enabled on the network.
- To test the District's service ticket submission process, we used our professional judgement to select a sample of three of the 17 unneeded employee user accounts and 10 of the 397 unneeded student accounts and requested the separation dates and service tickets that were submitted to the LHRIC to determine whether officials submitted tickets in a timely manner after the student or employee separated from the District.

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 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

[osc.ny.gov](https://www.osc.ny.gov)

