New York State Comptroller
THOMAS P. DiNAPOLI

West Hempstead Union Free School District

Nonstudent Network User Account Controls

2023M-9 | July 2023

Division of Local Government and School Accountability

Contents

Report Highlights

West Hempstead Union Free School District

Audit Objective

Determine whether West Hempstead Union Free School District (District) officials established adequate controls over nonstudent network user accounts to help prevent unauthorized use, access and loss.

Key Findings

District officials did not establish adequate controls over nonstudent network user accounts to help prevent unauthorized use, access and loss. In addition to sensitive information technology (IT) control weaknesses that were communicated confidentially to officials, we found that the Board of Education (Board) and District officials did not:

- Develop and adopt policies and procedures addressing key network user access controls, such as user account management, password security and user account controls.
- Disable 60 of the District's enabled nonstudent network accounts (11 percent) that were not needed. Twenty-two of these accounts (37 percent) have not been used in more than five years, with the oldest being last used more than 10 years ago. These accounts include:
    - 53 former employee network accounts, and
    - 7 network service accounts used for hardware devices and email aliases.

Key Recommendations

- Adopt comprehensive network user account policies and procedures addressing securing user accounts with passwords and adding, disabling and changing user access.
- Periodically review user access for all nonstudent network user accounts and disable user accounts when access is no longer needed.

District officials disagreed with certain aspects of our findings and recommendations, but indicated they have initiated or plan to initiate corrective action. Appendix B includes our comments on issues raised in the District's response letter.

Background

The District is located in the Town of Hempstead in Nassau County.

The Board is composed of seven-elected members and is responsible for the general management and control of the District's financial and educational duties. 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 Technology Director (Director) is responsible for oversight of the IT department and working with the Board to establish controls over the District's nonstudent network user accounts.

Quick Facts

Enabled Nonstudent Network User Accounts	
Teacher	383
Administrative	109
Business Office	65
Total	557

Audit Period

July 1, 2020 – May 26, 2022

Nonstudent Network User Account Controls

How Should District Officials Establish Controls Over Nonstudent Network User Accounts?

IT security policies define the tools and procedures used to help protect IT systems and define a school district board's expectations for appropriate user behavior. Therefore, it is essential for a board to adopt security policies for key network access controls to help safeguard against unauthorized access, use and loss. Policies directing IT officials to develop user account access controls while providing for appropriate management of the network user accounts are essential for effective IT governance.

Network user accounts provide access to resources on a network and are managed centrally by a server such as a domain controller. To minimize the risk of unauthorized access, officials should manage network user accounts and disable unnecessary accounts when they are no longer needed. To minimize the risk of unauthorized access, school district officials should maintain a list of authorized user accounts (identify users and accounts) and regularly compare enabled network user accounts to the current master payroll to ensure they are still needed.

School district officials should limit the use of shared and service network user accounts because they are not linked to one individual and officials may not be able to hold users accountable for their actions when using these accounts. Shared user accounts have usernames and passwords that are shared among two or more users and are often used to provide access to guests or other temporary or intermittent users. IT staff often use service accounts to run particular network or system services or applications (e.g., automated backup systems). School district officials should routinely evaluate the need for these accounts and disable those that are not related to a current district or system need. 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, make unauthorized changes to district records or deny legitimate access to network resources.

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction – or disruption of access of use – could have or cause a severe impact on critical functions, employees, students, third parties or other individuals or entities.

The Board Did Not Adopt Policies and Procedures Addressing Key Network User Account Controls

The Board did not adopt IT security policies and procedures to help secure network account user access, such as password security, user account management and user access controls. As a result, the Board did not provide sufficient guidance to officials and employees to help safeguard District IT systems and data. Consequently, IT assets accessible by these accounts were at risk for unauthorized access and loss and the District could incur a potentially costly disruption of operations and services.

While comprehensive policies will not guarantee the safety of IT systems, the lack of appropriate policies and procedures significantly increases the risk users will not understand their responsibilities, putting the data and computer resources they have been entrusted with at a greater risk for unauthorized access, misuse or abuse, and loss.

District Officials Did Not Adequately Manage Nonstudent Network User Accounts

The District relied on its nonstudent network user accounts for Internet access, email and maintaining confidential and sensitive financial and personnel records. As of May 26, 2022, the District had 557 enabled nonstudent network user accounts, including 383 teacher accounts, 109 administrative[2] accounts and 65 business office accounts. The District also maintained 459 computer accounts.[3]

We reviewed the District's 557 enabled nonstudent user accounts and identified 182 user accounts that did not match employees on the District's current payroll. Based on our discussion with the Director, we identified 53 enabled network account users that were for individuals no longer employed by the District. The Director told us that he disabled these 53 accounts as of September 13, 2022 as a result of our audit inquiry. The Director said that the IT department adds, changes or disables a user account when they receive an email from the Personnel Clerk advising that a new employee is hired, a change of access is necessary or an employee is separating from the District. The Director told us that these 53 user accounts were reactivated by the IT department to reclaim data from the user accounts and the IT department did not disable the accounts once the data was recovered, resulting in the unnecessary enabled user accounts. We

[2] In this usage, administrative refers to accounts utilized by District administration officials, such as principals, administrators and Board members.

[3] Computer accounts function as internal records within a network and allow IT administrators to manage computers.

identified user accounts that have not been logged into for several years, with the oldest dating back to October 4, 2012 (Figure 1). The Director should have disabled these accounts after reclaiming the data.

During our review, we also identified seven service network user accounts used for hardware devices, such as accessing the school billboard or a camera system, and email aliases that were no longer used by the District but had not been disabled. The Director informed us that he disabled these seven network service accounts on September 1st, 2022 and September 13, 2022. The remaining 122 network user accounts that did not agree to the current payroll were needed for appropriate District purposes, including user accounts for Board members (not on the District's payroll), employees with a legal name change, automated processes, hardware devices and email aliases.

Figure 1: User Accounts Last Logged In

Year(s)	User Accounts
5+	22
3-5	17
2-3	5
1-2	5
Less than 1	4

Overall, 60 nonstudent network user accounts were no longer necessary and allowed to remain enabled on the District's network because the IT department did not disable user accounts as soon as they became unneeded and did not perform an annual review of enabled nonstudent network user accounts. Without a periodic review and comparison of authorized network users to enabled network user accounts, unnecessary network user accounts were not identified by the IT department.

Unneeded nonstudent network user accounts are additional entry points into a network and, if accessed by an attacker, could severely disrupt District operations or be used to inappropriately access the District's network to view and/or remove personal information; make unauthorized changes to District records; or deny legitimate access to the District's network and records. When an organization has many network user accounts that must be managed and reviewed, unneeded nonstudent network user accounts increase the risk of inappropriate access by users with malicious intent.

What Do We Recommend?

The Board should:

1. Adopt comprehensive written IT policies addressing areas key to network user access, such as password security and controls over user account access.

2. Adopt comprehensive written policies and procedures for managing network user accounts, including adding, disabling and changing user access.

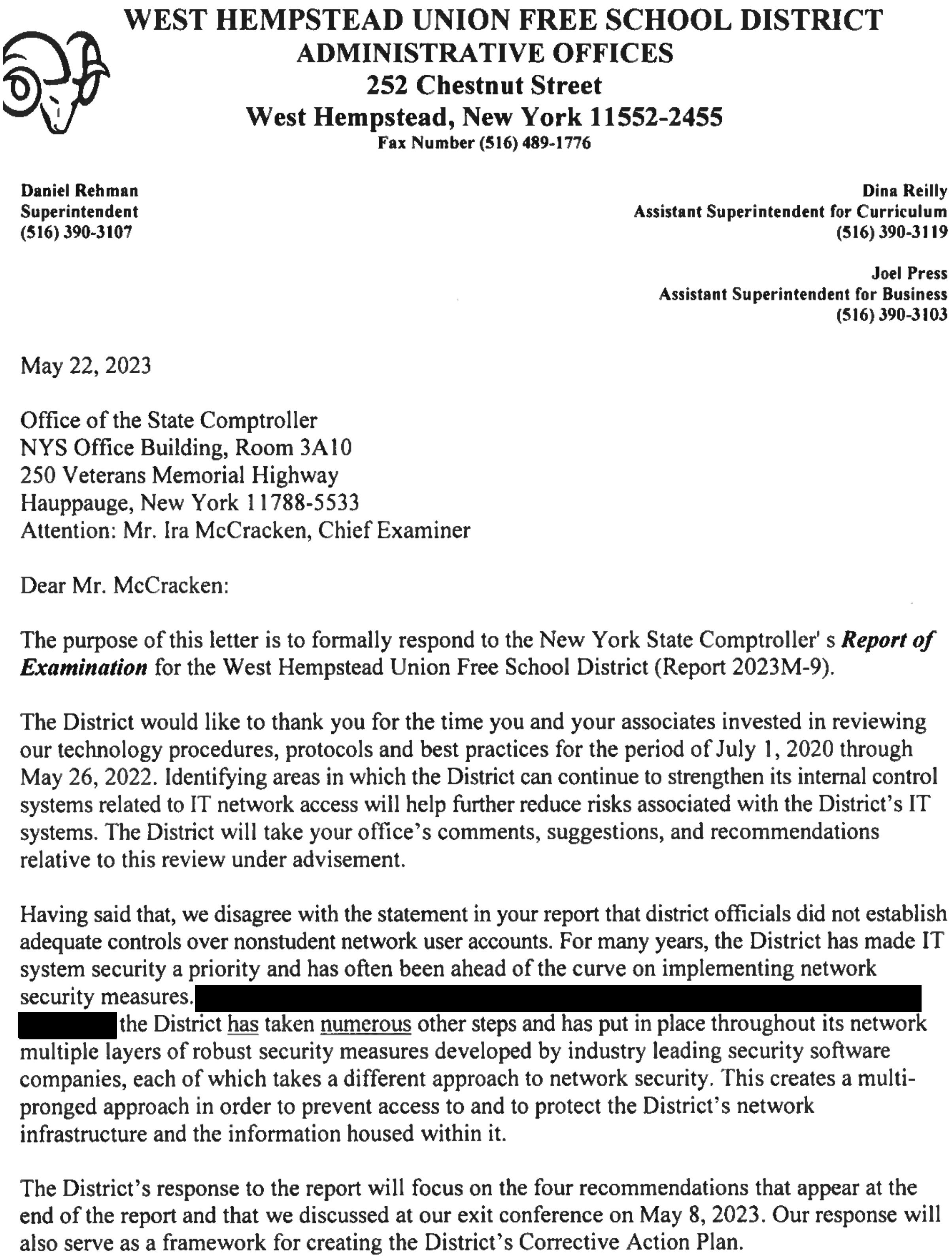
The Director should:

3. Disable network user accounts of employees as soon as they leave District employment and disable other unneeded nonstudent network user accounts in a timely manner.

4. Perform a periodic review of enabled nonstudent network user accounts to limit user accounts to those deemed necessary for District operations. In the event an account is reactivated to recover data, it should be immediately disabled once the data is recovered.

Appendix A: Response From District Officials

Portions of the District's response were redacted for security concerns.



WEST HEMPSTEAD UNION FREE SCHOOL DISTRICT
ADMINISTRATIVE OFFICES
252 Chestnut Street
West Hempstead, New York 11552-2455
Fax Number (516) 489-1776

Daniel Rehman
Superintendent
(516) 390-3107

Dina Reilly
Assistant Superintendent for Curriculum
(516) 390-3119

Joel Press
Assistant Superintendent for Business
(516) 390-3103

May 22, 2023

Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
Attention: Mr. Ira McCracken, Chief Examiner

Dear Mr. McCracken:

The purpose of this letter is to formally respond to the New York State Comptroller' s ***Report of Examination*** for the West Hempstead Union Free School District (Report 2023M-9).

The District would like to thank you for the time you and your associates invested in reviewing our technology procedures, protocols and best practices for the period of July 1, 2020 through May 26, 2022. Identifying areas in which the District can continue to strengthen its internal control systems related to IT network access will help further reduce risks associated with the District's IT systems. The District will take your office's comments, suggestions, and recommendations relative to this review under advisement.

Having said that, we disagree with the statement in your report that district officials did not establish adequate controls over nonstudent network user accounts. For many years, the District has made IT system security a priority and has often been ahead of the curve on implementing network security measures. [redacted] the District has taken numerous other steps and has put in place throughout its network multiple layers of robust security measures developed by industry leading security software companies, each of which takes a different approach to network security. This creates a multi-pronged approach in order to prevent access to and to protect the District's network infrastructure and the information housed within it.

See
Note 1
Page 9

The District's response to the report will focus on the four recommendations that appear at the end of the report and that we discussed at our exit conference on May 8, 2023. Our response will also serve as a framework for creating the District's Corrective Action Plan.

<u>Comptroller's Recommendation Number One</u>:
The Board of Education should adopt comprehensive written IT policies addressing areas key to network user access, such as password security and controls over user account access.

<u>District Response</u>:
The District subscribes to New York State School Boards Association's (NYSSBA) School Policy Update service. This service updates member districts quarterly on new laws and regulations that need to be incorporated into member districts' policy manuals. As part of this service, NYSSBA emails annotated sample policies and, when recommended, regulations so tha member districts can modify them and prepare final policies for adoption by the Board of Education. The District will utilize the NYSSBA Policy Update service and will work with District counsel and the Director of Technology to implement written IT policies addressing the Comptroller's recommendation.

<u>Comptroller' s Recommendation Number Two:</u>
The Board of Education should adopt comprehensive written policies and procedures for managing network user accounts, including adding, disabling and changing user access.

<u>District Response</u>:
Similar to the District's response to Recommendation Number One, the District will utilize the NYSSBA Policy Update service and will work with District counsel and the Director of Technology to adopt comprehensive written policies and procedures for managing network user accounts, including adding, disabling and changing user access.

<u>Comptroller's Recommendation Number Three:</u>
The District's IT Director should disable network user accounts of employees as soon as they leave District employment and disable other unneeded nonstudent network user accounts in a timely manner.

<u>District Response</u>:
The District <u>does</u> disable network user accounts of former employees as soon as they leave District employment. The District provided documentation to that effect to the Comptroller's office for 25 of the 53 instances cited in the Comptroller's report. The District occasionally need to reactivate previously disabled accounts in order to retrieve information from those accounts. [redacted]. In the cases cited by the Comptroller, the District did not disable those reactivated accounts in a timely manner. The District has now disabled those accounts. The District will put in place procedures to monitor and disable in a timely manner: (i) accounts of employees who have left District employment, (ii) shared and service user accounts, and (iii) any previously inactivated accounts that have been reactivated in order to retrieve data once the data is recovered. The District also plans to implement a software solution that will automatically disable user accounts when an employee is made inactive in the District's financial software system.

See
Note 2
Page 9

Comptroller's Recommendation Number Four:
Perform a periodic review of enabled nonstudent network user accounts to limit user accounts to those deemed necessary for District operations. In the event an account is reactivated to recover data, it should be immediately disabled once the data is recovered.

District Response
The Personnel Clerk notifies the Technology Department of an employee's change of status via email. The Technology department then disables the employee's network access. As mentioned in our response to Recommendation Number Three, the District also plans to implement a software solution that will automatically disable user accounts when an employee is made inactive in the District's financial software system. The District is also in the process of creating a systematic approach for periodically reviewing network user accounts to limit active user accounts to those deemed necessary for District operations. In the event that the District reactivates a previously disabled account in order to recover data, the District will immediately disable that account once the District has recovered all necessary data.

We would like to thank you for the opportunity to respond to your audit findings. The staff from your office who conducted the audit were courteous, respectful, and professional in their interactions with District personnel.

Please let me know if you a have any questions regarding this submission. Once this response is accepted, we will begin preparing the Corrective Action Plan with the appropriate and required specificity.

Best regards,

Daniel Rehman
Superintendent of Schools

Appendix B: OSC Comments on the District's Response

Note 1

While the District had established some IT controls over nonstudent network accounts, the District's lack of policies addressing password security and user account access, along with the lack of procedures requiring the disabling of user accounts as soon as they become unneeded, has resulted in unneeded nonstudent accounts remaining active over time, increasing the risk of unauthorized access, disruption or attack.

Note 2

The documents provided by the District demonstrate that the Personnel Clerk contacted the Director upon the separation of 25 of the 53 District employees; however, it does not support that the accounts for these employees were disabled by the Director either immediately upon separation from District employment or within a reasonable time after the accounts were reactivated for administrative purposes.

Appendix C: 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 interviewed the Director and reviewed District policies to gain an understanding of the District's controls over nonstudent network accounts. We inquired about IT policies and procedures for user access security.
- We used a computerized audit script, which we ran on May 26, 2022, to examine the District's domain controller and analyze the data to assess the necessity and appropriateness of network user accounts. We reviewed all 557 enabled nonstudent network user accounts to determine whether IT officials had adequately managed user accounts. We compared these 557 nonstudent network user accounts with the District's current master payroll to determine whether users were employed by the District.

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 D: 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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties