New York State Comptroller
THOMAS P. DiNAPOLI

Uniondale Union Free School District

Information Technology

2023M-61 | October 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Uniondale Union Free School District

Audit Objective

Determine whether Uniondale Union Free School District (District) officials adequately managed nonstudent network user accounts and permissions.

Key Findings

District officials did not adequately manage nonstudent network user accounts and permissions. 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 were confidentially communicated to officials, we found that the Technology Supervisor did not:

- Establish written procedures for granting, changing and disabling nonstudent network user account access, and regularly review the accounts to ensure they are necessary.
- Disable 3,471, or 71 percent, of the District's enabled nonstudent network user accounts that were not needed, including:
  - 1,824 individual user accounts, 515 of which were last used to log in to the network in 2003,
  - 1,647 shared and service user accounts, and
  - 12 network user accounts that had administrative permissions.

Key Recommendations

- Develop and adhere to written procedures for granting, changing and disabling nonstudent network user account access.
- Evaluate existing nonstudent network user accounts and disable them when access is no longer needed.

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

Background

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

The Board of Education (Board) is composed of five 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 Technology Supervisor is responsible for the oversight of the IT department with five staff members, including the system engineer, and ensuring nonstudent network user accounts are managed adequately.

Quick Facts

Enabled Nonstudent Network User Accounts	
Service and Shared Accounts	1,650
Individual Accounts	3,210
Total	**4,860**
Unneeded Nonstudent Network User Accounts	3,471

Audit Period

July 1, 2020 – May 26, 2022

Nonstudent Network User Accounts

How Should Officials Manage Nonstudent Network User Accounts and Permissions?

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 district records or deny legitimate access to network resources.

School district officials should develop and implement written procedures for granting, changing and disabling nonstudent network user account access to the network. Procedures should establish a process for revoking access by immediately disabling unneeded nonstudent network user accounts when they are no longer needed. To minimize the risk of unauthorized network use, access and loss, school district officials should actively manage nonstudent network user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are needed. When nonstudent network user accounts are no longer needed, they should be disabled in a timely manner. One way to help accomplish this is to establish and implement a system in which nonstudent network user accounts are automatically disabled after a reasonable specified period without a valid user account login, unless explicitly authorized to remain enabled on the network for an ongoing district or system need. In addition, school district officials should regularly review enabled nonstudent network user accounts to ensure they are still needed and disable unnecessary or unneeded user accounts when they are no longer 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 the accounts and disable those that are not related to a current district or system need.

School district officials should also regularly review administrative accounts and disable them when they are no longer needed. Generally, a network administrative account has permissions to monitor and control a network,

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

computers and applications and the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Officials Did Not Adequately Manage Nonstudent Network User Accounts and Permissions

District officials did not adequately manage nonstudent network user accounts and permissions for individual, shared and service accounts. The Technology Supervisor did not establish written procedures for granting, changing and disabling network user account access. In addition, although the IT department is in charge of managing the District's network, including nonstudent network user accounts, it did not independently verify or actively manage enabled nonstudent network user accounts to minimize the risk of unauthorized use, access and loss.

The IT department relied on the Human Resources (HR) department to notify them of changes in employment status for individual appointments, separations and transfers using a shared document. Upon receipt of this notification, the Technology Supervisor or system engineer would create, disable or make the applicable adjustment to the employee network user account.[2] However, this shared document was implemented in July 2021 and only began tracking changes in employment status for District employees in August 2021. Any changes prior to August 2021 were not captured in the District's shared document, as there was no plan or process in place to track changes in employment status prior to that date.

In addition, the IT department did not have procedures to establish and monitor enabled shared and service accounts, or to disable those deemed unnecessary. The Technology Supervisor and system engineer told us that shared and service accounts were created by IT staff as needed. For instance, they created shared accounts for student devices because a representative from the IT service provider indicated that certain shared user accounts were necessary for updates when the devices were initially implemented. However, because the IT department did not track shared accounts, the user accounts created for the student devices were not disabled when they were no longer needed. The Technology Supervisor and system engineer told us that as of December 2022, the District no longer used shared accounts. Similar to shared accounts, service accounts created by IT staff were not tracked. As a result, the IT department did not periodically monitor and disable unnecessary service accounts when they were no longer needed.

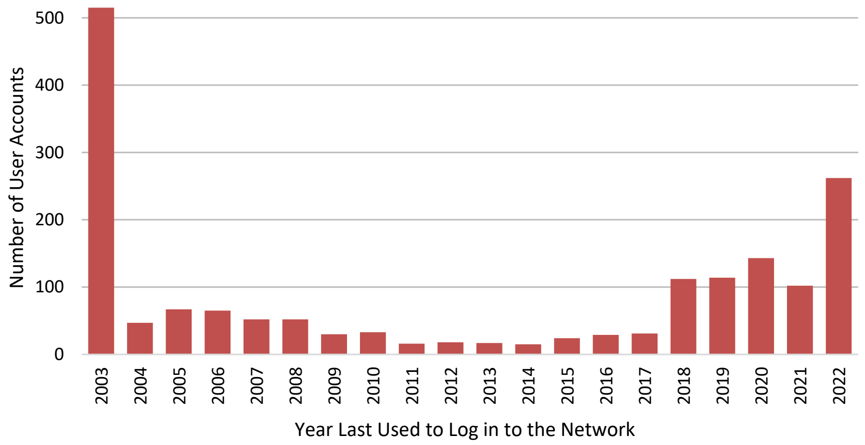
[2] The Technology Supervisor is responsible for managing teachers' network user accounts. The system engineer is responsible for managing non-teacher employee network user accounts.

We ran a computerized audit script in May 2022 and determined that the District had 4,860 enabled nonstudent network user accounts, including 3,210 individual accounts and 1,650 shared and service accounts. We reviewed all 4,860 enabled nonstudent network user accounts and determined that 3,471 user accounts (71 percent) were unneeded and should have been disabled. In addition, we determined that 12 user accounts had unnecessary administrative permissions.

Unneeded Individual Network User Accounts – We reviewed all 3,210 enabled individual nonstudent network user accounts and determined that 1,824 individual user accounts (57 percent) were unneeded and should have been disabled. Additionally, 1,743 of these 1,824 user accounts were not assigned to an individual listed as an active District employee. When we inquired about these user accounts, the system engineer could not explain why the 1,743 accounts were not assigned to an active District employee and indicated that they are likely user accounts of separated employees that have not been disabled. We analyzed 47 of these 1,743 user accounts and determined that nine were not assigned to prior employees. One account, created in 2006, was used by an independent contractor that previously provided grant writing services to the District and was last used to access the network in February 2010. The system engineer indicated that eight other user accounts were not associated with prior employees and because they were created by previous IT staff, he did not know why the accounts were created. All eight user accounts were created in 2013 or earlier, including four created in 2003, and were never used to log in to the District's network. The remaining 38 accounts were assigned to former employees that separated from the District between August 2003 and February 2022. In addition, 515 of the 1,743 accounts (30 percent) were last used to log in to the network in 2003, indicating that IT officials did not disable unneeded user accounts for up to 19 years (Figure 1).

FIGURE 1

Nonstudent User Accounts Last Used



Additionally, there were 81 enabled and unnecessary duplicate network accounts for users who already had an enabled nonstudent network user account. The system engineer said that these 81 accounts were duplicated because the IT department did not know that the users who requested access to a specific software already had a network user account. This occurred because District officials did not periodically review nonstudent network user accounts to determine whether any are unnecessary and should be disabled. Conducting periodic reviews of all network user accounts to determine whether accounts are necessary would help to identify unnecessary accounts, including duplicate accounts, and disable them in a timely manner.

Unneeded Shared and Service Accounts – We reviewed all 1,650 shared and service network user accounts and determined that 1,647 accounts (1,605 shared accounts and 42 service accounts), more than 99 percent, were unneeded and should have been disabled. This occurred because IT officials did not establish a process to monitor shared and service accounts to determine whether any are unnecessary and should be disabled. The system engineer indicated that all 1,647 accounts were not necessary and should have been disabled. Officials provided us with examples of why 1,440 of these accounts were not necessary:

- 1,292 shared accounts were assigned to student devices and created to send updates to the devices. These shared accounts should have been disabled because the District's mobile device management system, implemented in July 2018, did not require these shared network user accounts. The Technology Supervisor and system engineer said that the shared accounts were not disabled because they were not monitored by IT staff.
- 61 shared accounts were created to provide adult education students access to District computer programs but should have been disabled because the adult education program is no longer active. The Technology Supervisor indicated that these accounts were last used to access the network in 2018.
- Officials could not explain the use or need for 87 enabled shared accounts and indicated that these accounts should have been disabled. The system engineer said these shared accounts may have been set up by a company that used to handle the District's IT network, but was unsure about why the accounts were ever needed.

Furthermore, during our review of the 4,860 enabled nonstudent network user accounts, we determined that 12 of the unneeded accounts had administrative permissions, including 11 service accounts and one individual account. The system engineer indicated that the 11 service accounts required administrative permissions when they were created because they were system service accounts. For example, one account was created for the server to authenticate wireless devices (e.g., laptops). However, the system engineer said that this account was no longer needed. Additionally, the one individual account was created for an employee that needed access to the District's software to schedule buses. However, this network account did not require administrative permissions and should not have been created that way. Additionally, the account should have been disabled in March 2020 when the employee separated from the District.

Because there were no written procedures in place for IT department staff to review network user accounts, unneeded accounts, including some with administrative permissions, were not identified by IT officials until our audit. The Technology Supervisor indicated that network user accounts were not reviewed prior to our audit because of the lack of procedures and responsibilities frequently changing within the IT department. However, given that 71 percent of the nonstudent network user accounts were unnecessary, had IT staff reviewed the enabled network user accounts, they would have identified unneeded accounts.

Unneeded network user accounts, including those with elevated administrative permissions, are additional entry points into a network and, if compromised by an attacker, could be used to inappropriately access the District's network to view and/or remove personal information accessible by that compromised network account; make unauthorized changes to District records; or deny legitimate access to the District network and records. An attacker could use these additional entry points to severely disrupt District operations by:

- Denying District employees access to information they need to perform their job duties.
- Installing malicious software that could cripple and/or completely shut down the District's network.
- Obtaining and publicly releasing PPSI if it were accessible to a compromised network user account, such as employee and student dates of birth, home addresses and social security numbers, which could be used to facilitate identity theft.

These events could have criminal, civil, regulatory, financial and reputational impacts on District operations. Additionally, when a school district has many enabled network user accounts that must be managed and reviewed, it could make unneeded account detection less timely and accounts could be inadvertently granted unneeded permissions.

What Do We Recommend?

The Technology Supervisor should:

1. Develop and adhere to written procedures for granting, changing and disabling nonstudent network user account access.

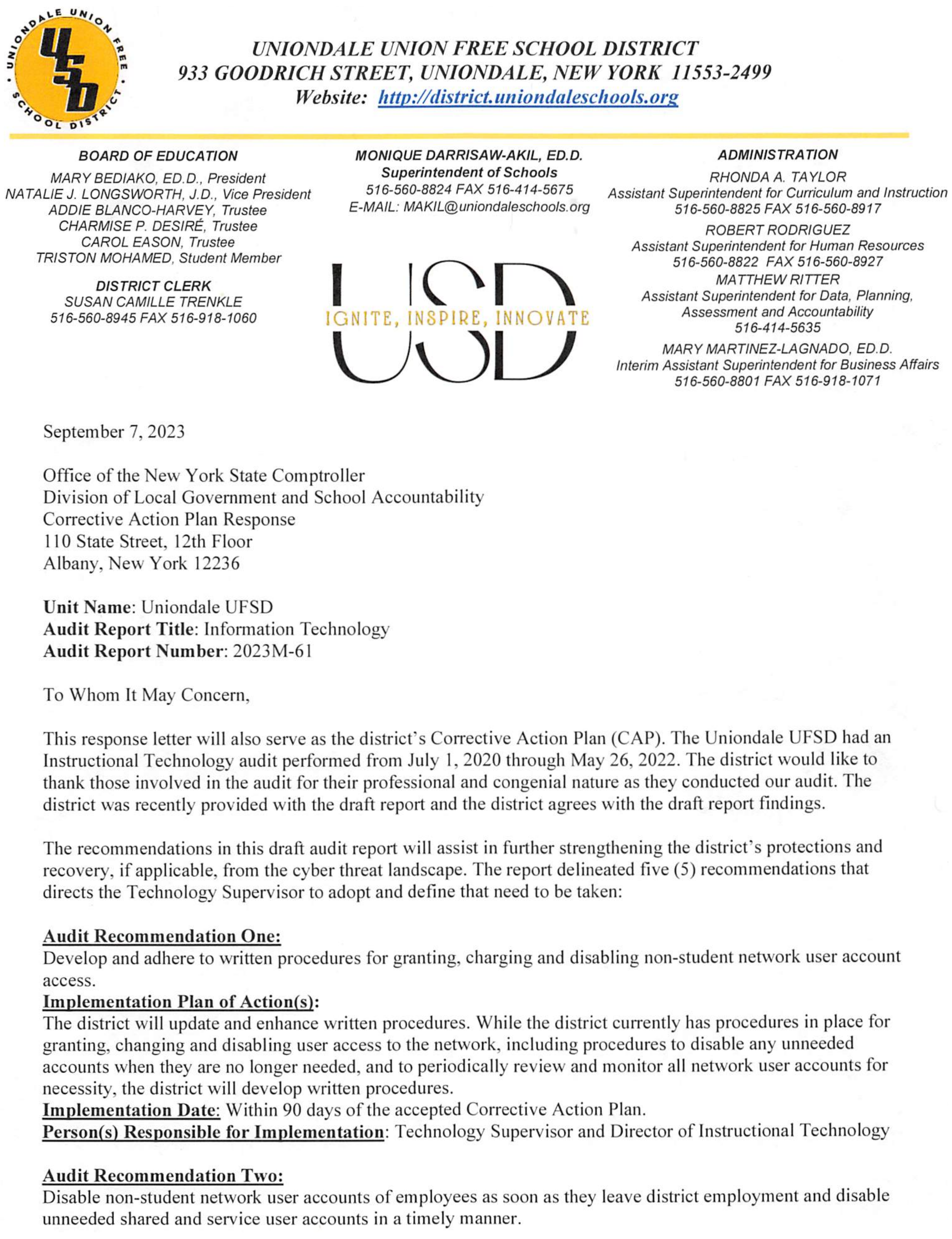
2. Disable nonstudent network user accounts of employees as soon as they leave District employment and disable unneeded shared and service user accounts in a timely manner.

3. Evaluate all current nonstudent network user accounts, including those with administrative permissions, and disable those that are unneeded.

4. Ensure effective procedures are in place to periodically review all nonstudent network user accounts for necessity and appropriateness.

5. Establish and implement a system in which network user accounts are disabled after a specified period of valid account login inactivity, unless authorized to remain enabled on the network for an ongoing District or system need.

Appendix A: Response From District Officials



UNIONDALE UNION FREE SCHOOL DISTRICT
933 GOODRICH STREET, UNIONDALE, NEW YORK 11553-2499
Website: http://district.uniondaleschools.org

DISTRICT CLERK
SUSAN CAMILLE TRENKLE
516-560-8945 FAX 516-918-1060

MONIQUE DARRISAW-AKIL, ED.D.
Superintendent of Schools
516-560-8824 FAX 516-414-5675
E-MAIL: MAKIL@uniondaleschools.org

ADMINISTRATION
RHONDA A. TAYLOR
Assistant Superintendent for Curriculum and Instruction
516-560-8825 FAX 516-560-8917
ROBERT RODRIGUEZ
Assistant Superintendent for Human Resources
516-560-8822 FAX 516-560-8927
MATTHEW RITTER
Assistant Superintendent for Data, Planning,
Assessment and Accountability
516-414-5635
MARY MARTINEZ-LAGNADO, ED.D.
Interim Assistant Superintendent for Business Affairs
516-560-8801 FAX 516-918-1071

September 7, 2023

Office of the New York State Comptroller
Division of Local Government and School Accountability
Corrective Action Plan Response
110 State Street, 12th Floor
Albany, New York 12236

Unit Name: Uniondale UFSD
Audit Report Title: Information Technology
Audit Report Number: 2023M-61

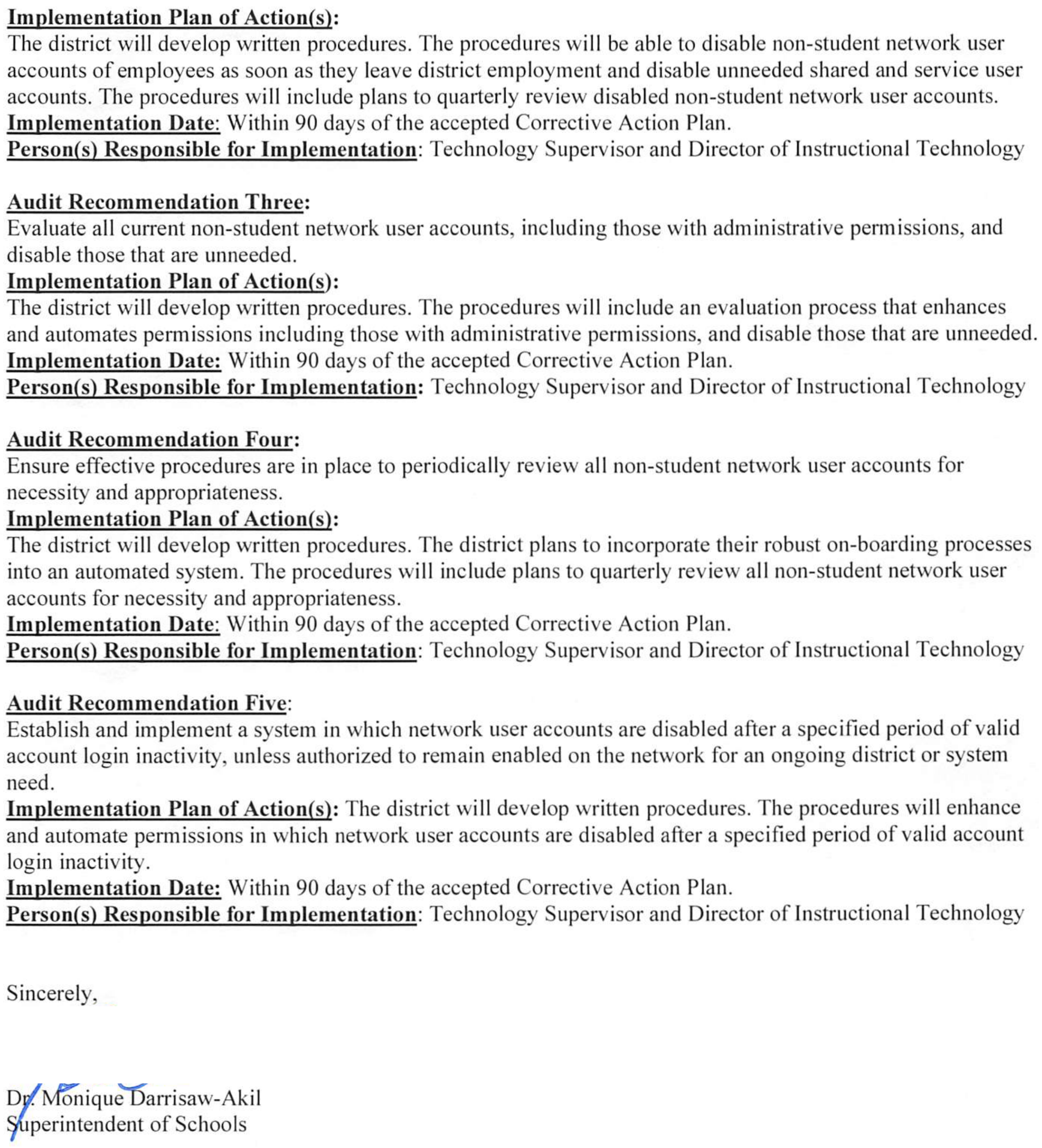
To Whom It May Concern,

This response letter will also serve as the district's Corrective Action Plan (CAP). The Uniondale UFSD had an Instructional Technology audit performed from July 1, 2020 through May 26, 2022. The district would like to thank those involved in the audit for their professional and congenial nature as they conducted our audit. The district was recently provided with the draft report and the district agrees with the draft report findings.

The recommendations in this draft audit report will assist in further strengthening the district's protections and recovery, if applicable, from the cyber threat landscape. The report delineated five (5) recommendations that directs the Technology Supervisor to adopt and define that need to be taken:

Audit Recommendation One:
Develop and adhere to written procedures for granting, charging and disabling non-student network user account access.
Implementation Plan of Action(s):
The district will update and enhance written procedures. While the district currently has procedures in place for granting, changing and disabling user access to the network, including procedures to disable any unneeded accounts when they are no longer needed, and to periodically review and monitor all network user accounts for necessity, the district will develop written procedures.
Implementation Date: Within 90 days of the accepted Corrective Action Plan.
Person(s) Responsible for Implementation: Technology Supervisor and Director of Instructional Technology

Audit Recommendation Two:
Disable non-student network user accounts of employees as soon as they leave district employment and disable unneeded shared and service user accounts in a timely manner.



Implementation Plan of Action(s):
The district will develop written procedures. The procedures will be able to disable non-student network user accounts of employees as soon as they leave district employment and disable unneeded shared and service user accounts. The procedures will include plans to quarterly review disabled non-student network user accounts.
Implementation Date: Within 90 days of the accepted Corrective Action Plan.
Person(s) Responsible for Implementation: Technology Supervisor and Director of Instructional Technology

Audit Recommendation Three:
Evaluate all current non-student network user accounts, including those with administrative permissions, and disable those that are unneeded.
Implementation Plan of Action(s):
The district will develop written procedures. The procedures will include an evaluation process that enhances and automates permissions including those with administrative permissions, and disable those that are unneeded.
Implementation Date: Within 90 days of the accepted Corrective Action Plan.
Person(s) Responsible for Implementation: Technology Supervisor and Director of Instructional Technology

Audit Recommendation Four:
Ensure effective procedures are in place to periodically review all non-student network user accounts for necessity and appropriateness.
Implementation Plan of Action(s):
The district will develop written procedures. The district plans to incorporate their robust on-boarding processes into an automated system. The procedures will include plans to quarterly review all non-student network user accounts for necessity and appropriateness.
Implementation Date: Within 90 days of the accepted Corrective Action Plan.
Person(s) Responsible for Implementation: Technology Supervisor and Director of Instructional Technology

Audit Recommendation Five:
Establish and implement a system in which network user accounts are disabled after a specified period of valid account login inactivity, unless authorized to remain enabled on the network for an ongoing district or system need.
Implementation Plan of Action(s): The district will develop written procedures. The procedures will enhance and automate permissions in which network user accounts are disabled after a specified period of valid account login inactivity.
Implementation Date: Within 90 days of the accepted Corrective Action Plan.
Person(s) Responsible for Implementation: Technology Supervisor and Director of Instructional Technology

Sincerely,

Dr. Monique Darrisaw-Akil
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 and procedures and interviewed the Technology Supervisor, system engineer, technology specialist and HR clerk to gain an understanding of nonstudent network user account management, specifically those related to granting, changing and disabling nonstudent user account access to the network.
- We examined nonstudent network user accounts and permissions using a computerized audit script run on May 26, 2022. We compared all 4,860 enabled nonstudent network user accounts to a current employee list. For the accounts that were not assigned to a specific employee, we followed up with the system engineer to determine the purpose of the account (i.e., shared accounts and service accounts). We analyzed the account login dates to identify unused and possibly unneeded nonstudent network user accounts.
- We followed up with the Technology Supervisor, system engineer and technology specialist to discuss possible unneeded nonstudent network user accounts and to determine why unneeded accounts remained enabled on the network.
- We compared usernames for a sample of user accounts to a list of separated employees to confirm whether the 1,743 unnecessary individual user accounts were for separated employees. We selected every 35th user account of the 1,743 for a total sample of 47 user accounts. Using our professional judgement, we determined that the sample of 47 user accounts was sufficient to corroborate the system engineer's assertion that the 1,743 user accounts were for separated employees.

Our audit also examined the adequacy of certain sensitive 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.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