New York State Comptroller
THOMAS P. DiNAPOLI

Bayport-Blue Point Union Free School District

Nonstudent Network User Accounts

2022M-190 | April 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Bayport-Blue Point Union Free School District

Audit Objective

Determine whether Bayport-Blue Point Union Free School District (District) officials established adequate nonstudent network user account controls.

Key Findings

District officials did not establish adequate network controls for nonstudent user accounts to help prevent unauthorized access. As a result, the District has an increased risk of unauthorized access to and use of the District network and potential loss of important data. In addition to sensitive information technology (IT) control weaknesses that were confidentially communicated to officials, we found the Database Coordinator did not:

- Disable 281 nonstudent network user accounts that are unneeded or unnecessary to prevent unauthorized access and use.

Key Recommendations

- Disable unneeded or unnecessary network user accounts as soon as they are no longer needed and regularly review network user accounts for necessity.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action. Appendix B includes our comments on issues raised in the District's response letter.

Background

The District, located in the Towns of Brookhaven and Islip in Suffolk County, is governed by an elected seven-member Board of Education (Board) responsible for the general management and control of financial and educational affairs.

The Superintendent of Schools (Superintendent) is the chief executive officer responsible, under the Board's direction, to establish regulations governing the use and security of the District's computer network. The Database Coordinator reports to the Assistant Superintendent for Finance and Operations and is responsible for the District's network including controlling access, disseminating policies, training and monitoring.

Quick Facts

Enabled Network User Accounts	
Student	3,301
Employee	897
Shared	37
Service	114
Total	4,349

Employees	860
Students	2,140

Audit Period

July 1, 2018 – April 15, 2021

Nonstudent Network User Accounts

School districts rely on networks to access and use IT assets and systems for a variety of tasks including storage of financial, student and personnel records, which contain personal, private and sensitive information (PPSI)[1] and/or personal identifiable information (PII);[2] email; and Internet access. These networks along with the accessed and used assets and systems are valuable and need to be protected from unauthorized access and use.

How Should School District Officials Establish Adequate Network User Access Account Controls?

Because user accounts provide access to the network, officials should actively manage them to minimize the risk of unauthorized use, access and loss. If not properly managed, unneeded user accounts may not be detected and disabled timely. Unneeded accounts are additional entry points for attackers to attempt to gain unauthorized access and then potentially use to inappropriately access and view PPSI, make changes to official school district records or deny legitimate access to electronic information when needed.

School district officials should establish written procedures for actively managing user accounts, including their creation, use and dormancy. User accounts should be disabled as soon as they are no longer needed, and regularly monitored to ensure they are appropriate and authorized. To accomplish this, an appropriate official should immediately notify the administrators when an account user's employment or contract is terminated so that the administrator can disable the user's accounts in all computer-related applications. Another way to accomplish this is to establish and implement a system in which network user accounts are disabled, either automatically or manually, after a reasonable specified period without a valid user account login.

Officials should limit the use of shared and service user accounts as they are not linked to one individual and therefore may have reduced accountability. Shared user accounts are accounts with usernames and passwords that are shared among two or more users and are often used to, for example, provide access to guests or other temporary or intermittent users. Service accounts are accounts created for the sole purpose of running a particular network or system service or application (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 school district or system need.

[1] PPSI is any information to which unauthorized access, disclosure, modification or destruction – 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.

[2] PII includes but is not limited to: information concerning a person which, because of name, number, personal mark or other identifier, can be used to identify a person, in combination with: Social Security number; driver's license number or non-driver identification card number; mother's maiden name; or financial account identifiers or other information which would permit access to a person's financial resources or credit.

Officials Did Not Establish Adequate Controls Over Nonstudent Network User Account Access

District officials did not establish adequate controls over nonstudent network user accounts for individual, shared or service accounts. They did not establish written procedures for granting, verifying, 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 verify or actively monitor nonstudent network user accounts to ensure they are necessary.

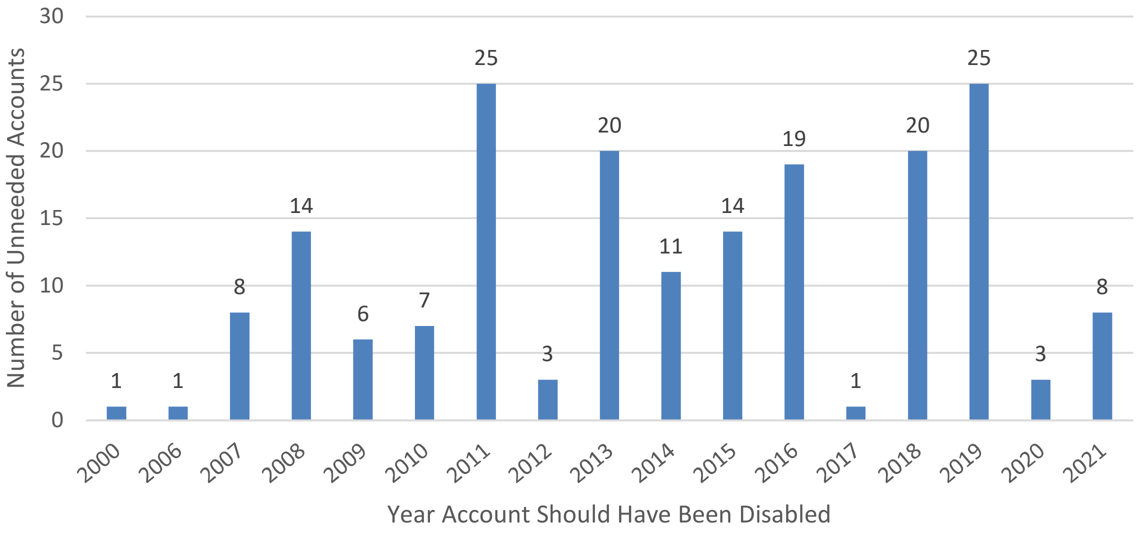
On March 30, 2021, the District had 1,048 nonstudent user accounts - 897 employee user accounts, 37 shared user accounts and 114 service user accounts. Over one-fourth of these nonstudent network accounts (281 of 1,048) were no longer necessary. These unnecessary accounts included those assigned to former staff, as well as unneeded shared and service accounts across the District network.

Over one-fourth of these nonstudent network accounts (281 of 1,048) were no longer necessary.

Former Employee Network User Accounts – More than 20 percent (186 of 897) of the enabled network user accounts were unneeded because they were assigned to employees no longer employed by the District. These former employees' accounts remained enabled and unused as far back as June 2000, more than 20 years ago (Figure 1). Also, 97 of the 186 accounts (52 percent) had a last login date after their employment termination date.

FIGURE 1

Former Employee Network User Accounts



The Database Coordinator told us the reason these accounts were not disabled was because the IT Department was never notified by the Personnel Director of the employee separations. She could not explain why they were not notified, but she did say there is a new Personnel Director who was appointed July 2019 that more regularly notifies the IT Department of staff changes. However, since July 2019, 18 employees separated from the District but still had a network user account at the time of our review. The Database Coordinator also said she does not have time to do a full review of user accounts to remove old, unneeded accounts so it is done little by little when she has time. In response to the accounts that had a login date after their termination date, the Database Coordinator stated that separated staff are often hired as substitutes or for part-time positions where their user account would be reactivated from its disabled state. Also, separated staff may request their account not to be disabled immediately in order to obtain files from their accounts. However, officials would rarely, if ever, have advance knowledge of a returning former employee. Therefore, network user accounts of former employees should be disabled as soon as they leave District employment. Further, allowing former staff to access files after their employment has ended is a significant risk and should not be permitted. She also indicated that the only risk would be that the separated staff could send emails. The separated staff would not be able to enter into any other program or system unless they were both onsite and logged into a District device. However, this is in contradiction to a previous assertion made by the Database Coordinator when she indicated that there are multiple individuals who have the ability to remotely access a system and/or device on the District network.

<u>Unneeded Shared and Service Accounts</u> – Nearly 60 percent (22 of 37) of the shared user accounts and nearly two-thirds (73 of 114) of the service accounts were unneeded and not necessary, based on our discussions with the Database Coordinator. After we discussed these accounts with IT Department staff, the 95 accounts were disabled.

The Database Coordinator said the reason these accounts were not disabled sooner is because the IT Department did not know there were any unneeded accounts, and the Department had no procedure to review user accounts for necessity.

The Board has adopted multiple IT policies; however, these policies do not address network user account management. Further, District officials did not develop written procedures for granting, changing and disabling network user accounts and the Database Coordinator does not regularly review enabled network user accounts to ensure that all user accounts are still needed.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could be used for unauthorized access to the District network to then view and/or remove personal information, make unauthorized changes to District records or deny legitimate access to the District's network and records. An attacker could use these additional entry points to severely disrupt District operations by:

- Denying District employees network access to electronic information they need to perform their job duties,
- Installing malicious software that could cripple and/or completely shut down the District network,
- Obtaining and publicly releasing PPSI, such as employee and student date of birth, home address and social security numbers, which could be used to facilitate identity theft, and
- Inappropriately accessing and changing District records, such as student grades.

These types of events would have criminal, civil, regulatory, financial and reputational impacts on District operations.

What Do We Recommend?

The Board should:

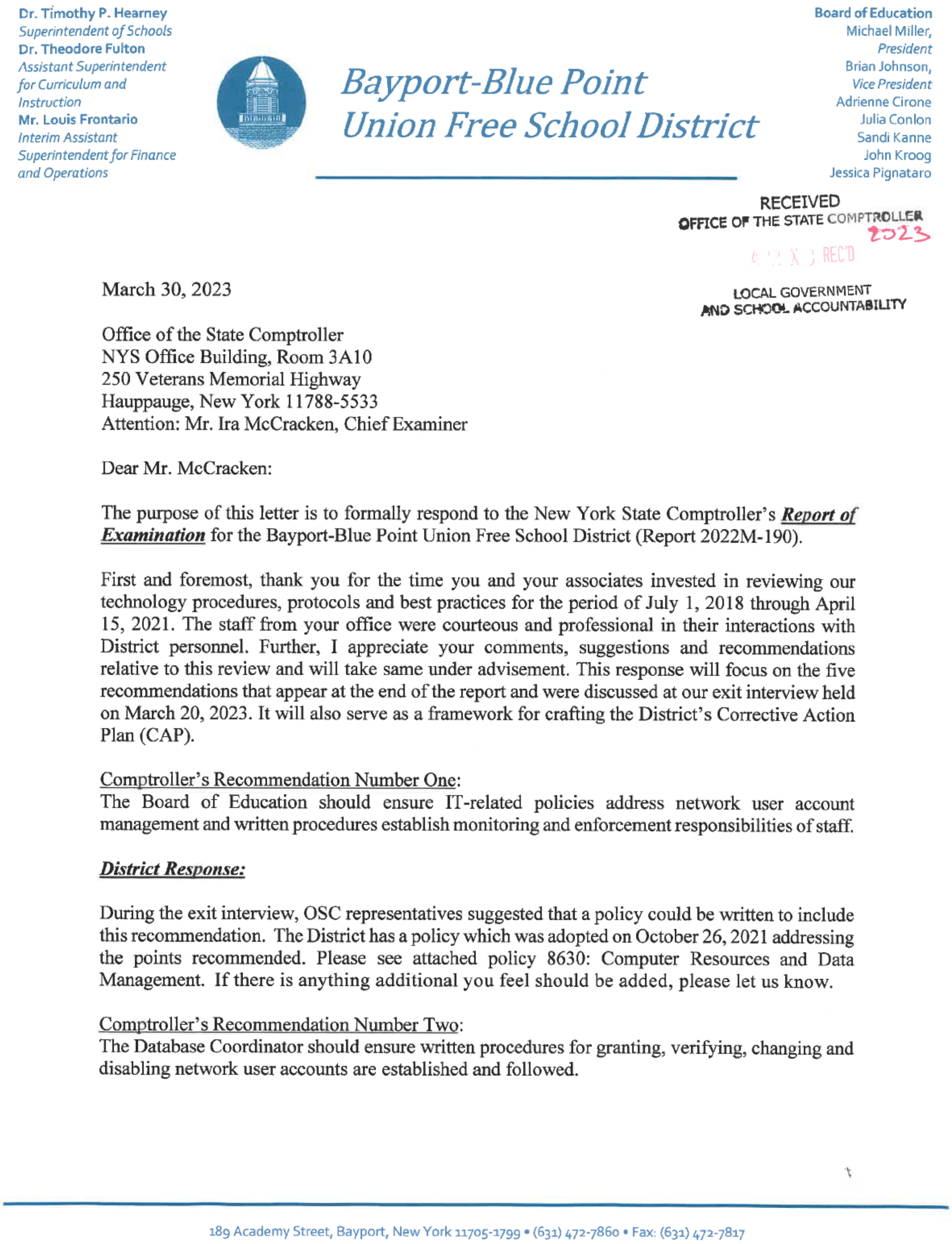
1. Ensure IT-related policies address network user account management and written procedures establish monitoring and enforcement responsibilities of staff.

The Database Coordinator should ensure:

2. Written procedures for granting, verifying, changing and disabling network user accounts are established and followed.
3. Network user accounts of former employees are disabled as soon as they leave District employment and disable shared and service user accounts as soon as they are no longer needed.
4. A system is established and implemented to disable network user accounts after a specified period of account inactivity.
5. A system to periodically review network user accounts is established to determine which are unnecessary and should be disabled.

Appendix A: Response From District Officials

The District's response letter refers to an attachment that supports the response letter. Because the District's response letter provides sufficient detail of its actions and the attachment contains details on District specific applications, we did not include the attachment in Appendix A.



Dr. Timothy P. Hearney
Superintendent of Schools
Dr. Theodore Fulton
Assistant Superintendent for Curriculum and Instruction
Mr. Louis Frontario
Interim Assistant Superintendent for Finance and Operations

Bayport-Blue Point
Union Free School District

Board of Education
Michael Miller,
President
Brian Johnson,
Vice President
Adrienne Cirone
Julia Conlon
Sandi Kanne
John Kroog
Jessica Pignataro

March 30, 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 Bayport-Blue Point Union Free School District (Report 2022M-190).

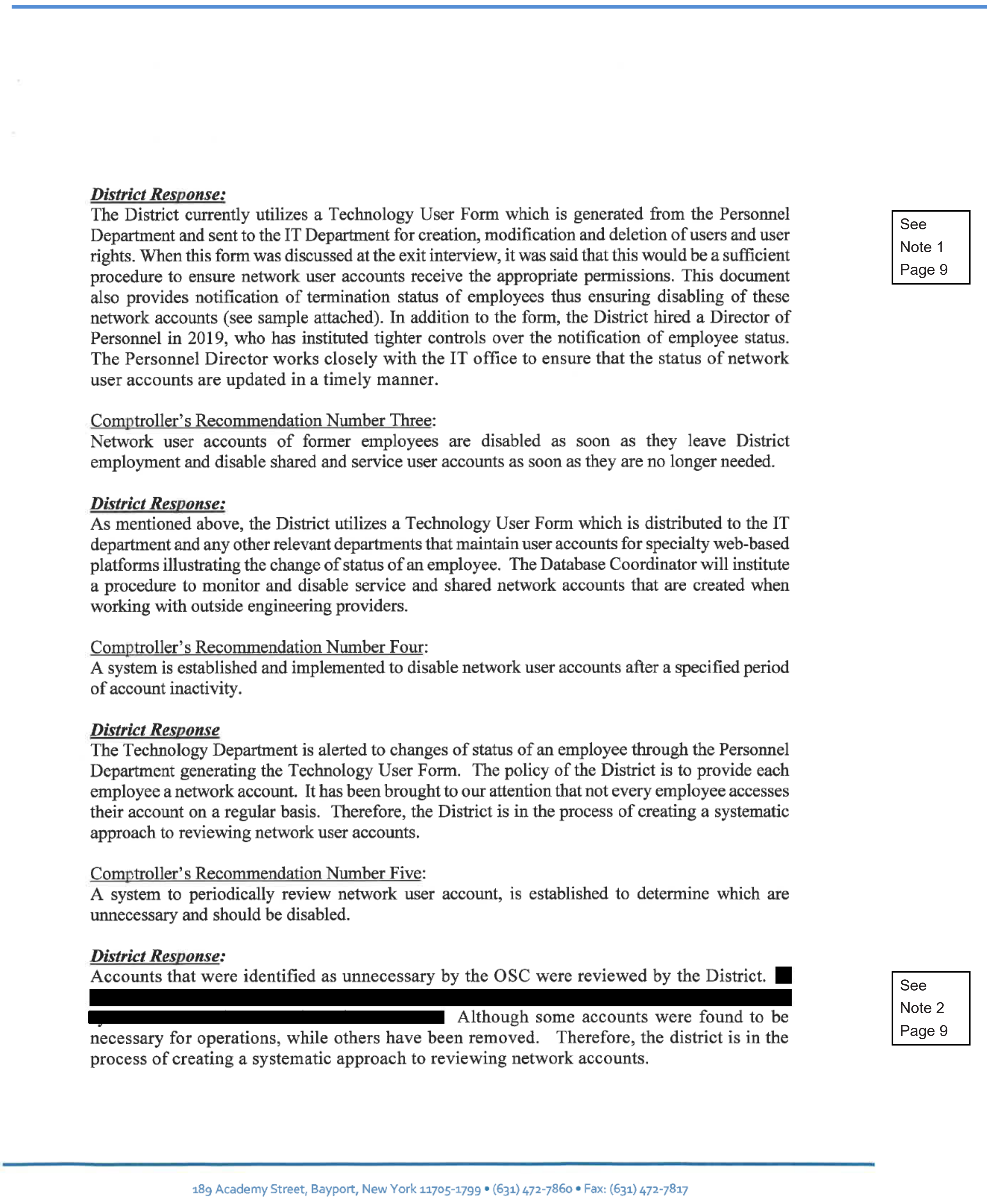
First and foremost, thank you for the time you and your associates invested in reviewing our technology procedures, protocols and best practices for the period of July 1, 2018 through April 15, 2021. The staff from your office were courteous and professional in their interactions with District personnel. Further, I appreciate your comments, suggestions and recommendations relative to this review and will take same under advisement. This response will focus on the five recommendations that appear at the end of the report and were discussed at our exit interview held on March 20, 2023. It will also serve as a framework for crafting the District's Corrective Action Plan (CAP).

Comptroller's Recommendation Number One:
The Board of Education should ensure IT-related policies address network user account management and written procedures establish monitoring and enforcement responsibilities of staff.

District Response:

During the exit interview, OSC representatives suggested that a policy could be written to include this recommendation. The District has a policy which was adopted on October 26, 2021 addressing the points recommended. Please see attached policy 8630: Computer Resources and Data Management. If there is anything additional you feel should be added, please let us know.

Comptroller's Recommendation Number Two:
The Database Coordinator should ensure written procedures for granting, verifying, changing and disabling network user accounts are established and followed.



District Response:
The District currently utilizes a Technology User Form which is generated from the Personnel Department and sent to the IT Department for creation, modification and deletion of users and user rights. When this form was discussed at the exit interview, it was said that this would be a sufficient procedure to ensure network user accounts receive the appropriate permissions. This document also provides notification of termination status of employees thus ensuring disabling of these network accounts (see sample attached). In addition to the form, the District hired a Director of Personnel in 2019, who has instituted tighter controls over the notification of employee status. The Personnel Director works closely with the IT office to ensure that the status of network user accounts are updated in a timely manner.

See
Note 1
Page 9

Comptroller's Recommendation Number Three:
Network user accounts of former employees are disabled as soon as they leave District employment and disable shared and service user accounts as soon as they are no longer needed.

District Response:
As mentioned above, the District utilizes a Technology User Form which is distributed to the IT department and any other relevant departments that maintain user accounts for specialty web-based platforms illustrating the change of status of an employee. The Database Coordinator will institute a procedure to monitor and disable service and shared network accounts that are created when working with outside engineering providers.

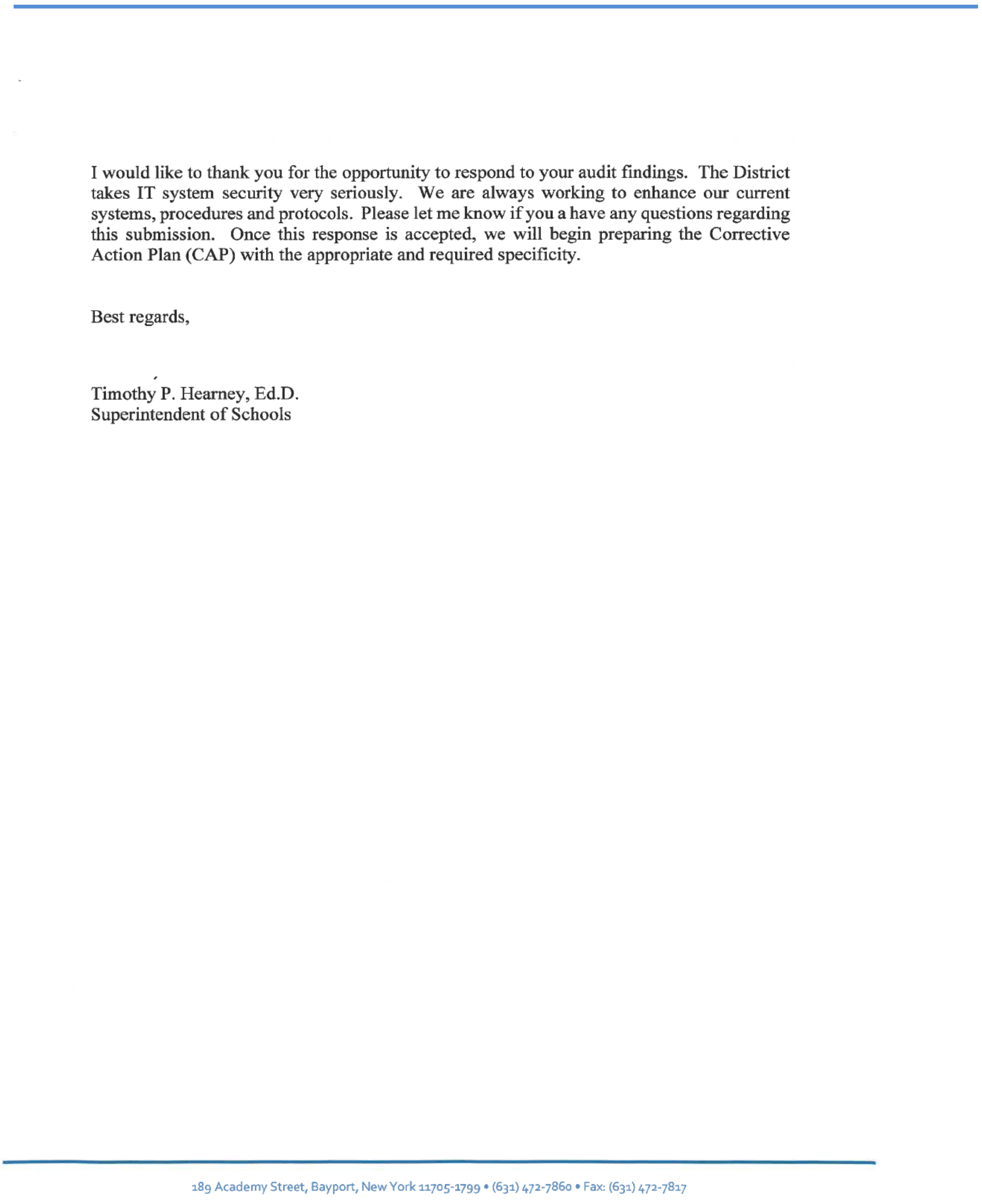
Comptroller's Recommendation Number Four:
A system is established and implemented to disable network user accounts after a specified period of account inactivity.

District Response
The Technology Department is alerted to changes of status of an employee through the Personnel Department generating the Technology User Form. The policy of the District is to provide each employee a network account. It has been brought to our attention that not every employee accesses their account on a regular basis. Therefore, the District is in the process of creating a systematic approach to reviewing network user accounts.

Comptroller's Recommendation Number Five:
A system to periodically review network user account, is established to determine which are unnecessary and should be disabled.

District Response:
Accounts that were identified as unnecessary by the OSC were reviewed by the District. [redacted] Although some accounts were found to be necessary for operations, while others have been removed. Therefore, the district is in the process of creating a systematic approach to reviewing network accounts.

See
Note 2
Page 9



I would like to thank you for the opportunity to respond to your audit findings. The District takes IT system security very seriously. We are always working to enhance our current systems, procedures and protocols. 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 (CAP) with the appropriate and required specificity.

Best regards,

Timothy P. Hearney, Ed.D.
Superintendent of Schools

Appendix B: OSC Comments on the District's Response

Note 1

At the exit conference, District officials indicated that they planned to update their Technology User Form (Form) to improve the procedures for network user account access management (e.g., grant, verify, change and disable). Although an updated Form was not provided for our review during the exit conference, based on the response letter, officials seem to be addressing the recommendation. However, in addition to employee accounts, the written procedures for granting, verifying, changing and disabling network user accounts should include both shared and service accounts.

Note 2

We redacted this sentence as it contained sensitive information.

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 reviewed IT-related policies and interviewed the Superintendent, Assistant Superintendent and the Database Coordinator and IT Department staff to gain an understanding of the network operations to access and use IT assets and systems and determine the adequacy of IT policies and procedures in safeguarding IT assets and systems.
- We inquired about written procedures for granting, verifying, changing and disabling network user accounts to determine whether the District is managing user accounts and ensuring user account access is necessary and appropriate.
- We analyzed network user accounts using a computerized audit script run on March 30, 2021. We compared the 1,048 non-student enabled network user accounts to a current employee list and interviewed the Database Coordinator regarding unused and other potentially unneeded accounts to identify unnecessary accounts.

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 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