New York State Comptroller
THOMAS P. DiNAPOLI

Whitney Point Central School District

Information Technology

2023M-179 | June 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Whitney Point Central School District

Audit Objective

Determine whether Whitney Point Central School District (District) officials adequately managed nonstudent network user accounts and developed and adopted a comprehensive information technology (IT) contingency plan.

Key Findings

District officials did not adequately manage nonstudent network user accounts, which are network user accounts not specifically assigned to a student (e.g., authorized staff, third-party vendors and shared accounts). Officials also did not adopt an IT contingency plan and were unaware of all the network users that had access to the District's network. When nonstudent network user accounts are not adequately managed and an IT contingency plan is not adopted, the District has an increased risk that it could suffer a serious interruption to operations due to the risk to the network and potential inability to communicate during a disruption.

In addition to sensitive IT control weaknesses that we confidentially communicated to officials, District officials did not disable 19 nonstudent network user accounts (4 percent) that were not needed and/or used in more than five years. All of these user accounts were subsequently deleted during our audit fieldwork.

Key Recommendations

- Develop written procedures for managing nonstudent network user accounts that include periodically reviewing user access and disabling unneeded and/or unused accounts.
- Adopt a comprehensive IT contingency plan, update the plan as needed and distribute it to all responsible parties.

District officials generally agreed with our recommendations and have indicated they planned to initiate corrective action. Appendix B includes our comment on an issue that was raised in the District's response letter.

Audit Period

July 1, 2021 – February 24, 2023. We extended our audit period to August 31, 2023 to review backup restoration results and November 16, 2023 to review updates to certain user accounts.

Background

The District serves 11 towns located in Broome, Chenango, Cortland and Tioga counties.

The District is governed by an elected seven-member Board of Education (Board), responsible for managing and controlling 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 District contracts with the Broome-Delaware-Tioga Board of Cooperative Educational Services South Central Regional Information Center (SCRIC) for managed IT and backup services. The Assistant Superintendent is the liaison between the District and SCRIC staff.

Quick Facts	
Nonstudent Network User Accounts Enabled and Reviewed	508
Full- and Part-Time Employees	460
2021-22 Managed IT and Backup Service Contract	$362,720

Information Technology

Network user accounts are necessary to allow authorized users access to resources on a server or computer on the network. Nonstudent network user accounts are network user accounts that are not specifically assigned to a student (e.g., authorized staff, third-party vendors and shared accounts)[1]. Although network user accounts can be set to limit access to only certain resources, they are additional entry points into a network and could be used to inappropriately access unauthorized data and information.

As part of the managed IT services contract, District employees and SCRIC staff managed nonstudent network user accounts that provided users with access to network resources and data needed to complete their job duties and responsibilities. Compromised nonstudent network user accounts could be used to inappropriately access and view personal, private and sensitive information (PPSI)[2] on the network, make unauthorized changes to official District records or deny legitimate access to network resources. Therefore, adequate nonstudent network user account management, in combination with a comprehensive IT contingency plan, is vital to protecting the network and data against IT and cybersecurity risks.

How Can Officials Ensure Only Needed Nonstudent Network User Accounts Are Enabled?

Effective management of network user accounts (e.g., staff, third-party vendor and shared accounts) involves establishing written procedures that guide network and/or system administrators in properly creating, granting, modifying and disabling user account access to a network. These procedures should specify roles and responsibilities of school district staff and IT vendors and require periodic monitoring of all enabled network user accounts to help IT staff determine whether the accounts are appropriate and needed.

All network user accounts should be disabled when they are no longer needed. School district officials should periodically review all network user accounts to determine whether they are necessary. Officials should identify any unused or infrequently used network user accounts (e.g., not used for six months or more) and determine whether they are necessary or should be enabled only when needed.

[1] Shared accounts are used by more than one user to log in to a computer system and access network resources. For example, shared accounts may be used for testing processes, training purposes or shared email accounts.

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

When possible, IT staff should establish a unique individual user account for each user to provide accountability. While managing nonstudent network user accounts, IT staff should limit the use of shared network user accounts because they are not linked to one individual, and users may not be held individually accountable for their actions when using these accounts. IT staff should routinely evaluate shared user accounts to determine whether they are needed.

Officials Did Not Ensure Only Needed Nonstudent Network User Accounts Were Enabled

We reviewed all 508 enabled nonstudent network user accounts with access to the District's network and identified 26 accounts (5 percent), including 22 shared user accounts and four individual user accounts, that were no longer needed and/or were not used in more than five years. District officials subsequently deleted 19 of these user accounts that were no longer needed and indicated the remaining seven user accounts were still needed.

Unused Shared Network User Accounts – We determined that 22 shared network user accounts were last used between five and 12 years ago. We discussed these accounts with District officials and verified that officials deleted 15 of these shared user accounts during our audit fieldwork. District officials provided us with reasonable explanations why the remaining seven shared user accounts were necessary for District operations.

Unnecessary Individual Nonstudent Network User Accounts – We determined that four individual network user accounts were unnecessary and should have been disabled. The individual network user accounts were assigned to three former employees and one former intern who have all separated from the District. The Assistant Superintendent said that one former employee user account had remained enabled because a current District employee needed temporary access to specific files used by the former employee. However, this practice diminished the accountability over, access to and use of this network account. The Assistant Superintendent agreed that the four user accounts were no longer needed, and we confirmed that District officials deleted the accounts during our audit fieldwork.

District officials established practices[3] to guide network and/or system administrators in creating, granting, modifying and monitoring (quarterly) District-related network user account access. However, the procedures did not include a process for reviewing all user accounts with access to the District's network (e.g., SCRIC-created user accounts) to determine whether they needed to be disabled. Additionally, the procedures did not have a timeline for when unused

[3] As part of the managed IT service contract, the SCRIC created, changed and disabled network user accounts based on District authorization. Periodically, the SCRIC provided a list of staff accounts for District officials to review.

accounts should be disabled. Furthermore, District officials could not provide the authorization needed by SCRIC to properly manage network user accounts because District officials were unaware of all user accounts with access to the network.

Unused and unnecessary network user accounts are additional entry points into a network and, if accessed by attackers, could be used to inappropriately access and view PPSI accessible by those accounts and potentially compromise IT resources.

Why Is a Comprehensive IT Contingency Plan Needed?

A comprehensive IT contingency plan helps minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. These events could include power outages, software or hardware failures caused by a virus or other type of malicious software (e.g., ransomware), human error, equipment destruction or a natural disaster (e.g., flood, fire). An IT contingency plan should be finalized, adopted by a school board and distributed to key individuals. The plan should include an analysis of business processes and continuity needs, identify roles of key individuals, contain necessary precautions to recover data and resume operations in the event of an unplanned disruption, and specify off-site and off-network data backup procedures. In addition, officials should periodically test and update the plan during and after a disruptive event, and distribute updates to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements, such as statutory changes.

The District Does Not Have an Approved IT Contingency Plan

Although District officials developed a draft IT contingency plan, it was not adopted by the Board. The Assistant Superintendent provided the draft plan to the audit team and based on our review, we determined that the plan was comprehensive and met the District’s needs. However, because the plan was in draft form and not presented to and reviewed by the Board, it was never adopted or distributed to key individuals. Therefore, in the event of a disruption or disaster – including a ransomware attack or other unplanned event – key officials and District staff did not have approved guidance to help guide them to recover data, resume essential operations in a timely manner and help minimize damage and recovery costs.

The Board contracted with SCRIC to perform select IT services, including daily backups of all data, applications and operating systems. These backups were encrypted and stored at a secure, off-site location. District officials said that backups were periodically restored, and we reviewed documentation confirming that the most recent restoration was successful. In lieu of an adopted plan, District officials told us they relied on the backup services provided by SCRIC to restore services in the event of a disruption or disaster.

District officials did provide some elements for their likely response to unplanned cyber events (e.g., backup procedures). However, without an adopted IT contingency plan that is distributed to key officials and staff, the District has an increased risk that it could suffer a serious interruption to operations because their ability to communicate during a disruption or disaster could affect the timely processing of business functions.

What Do We Recommend?

District officials should:

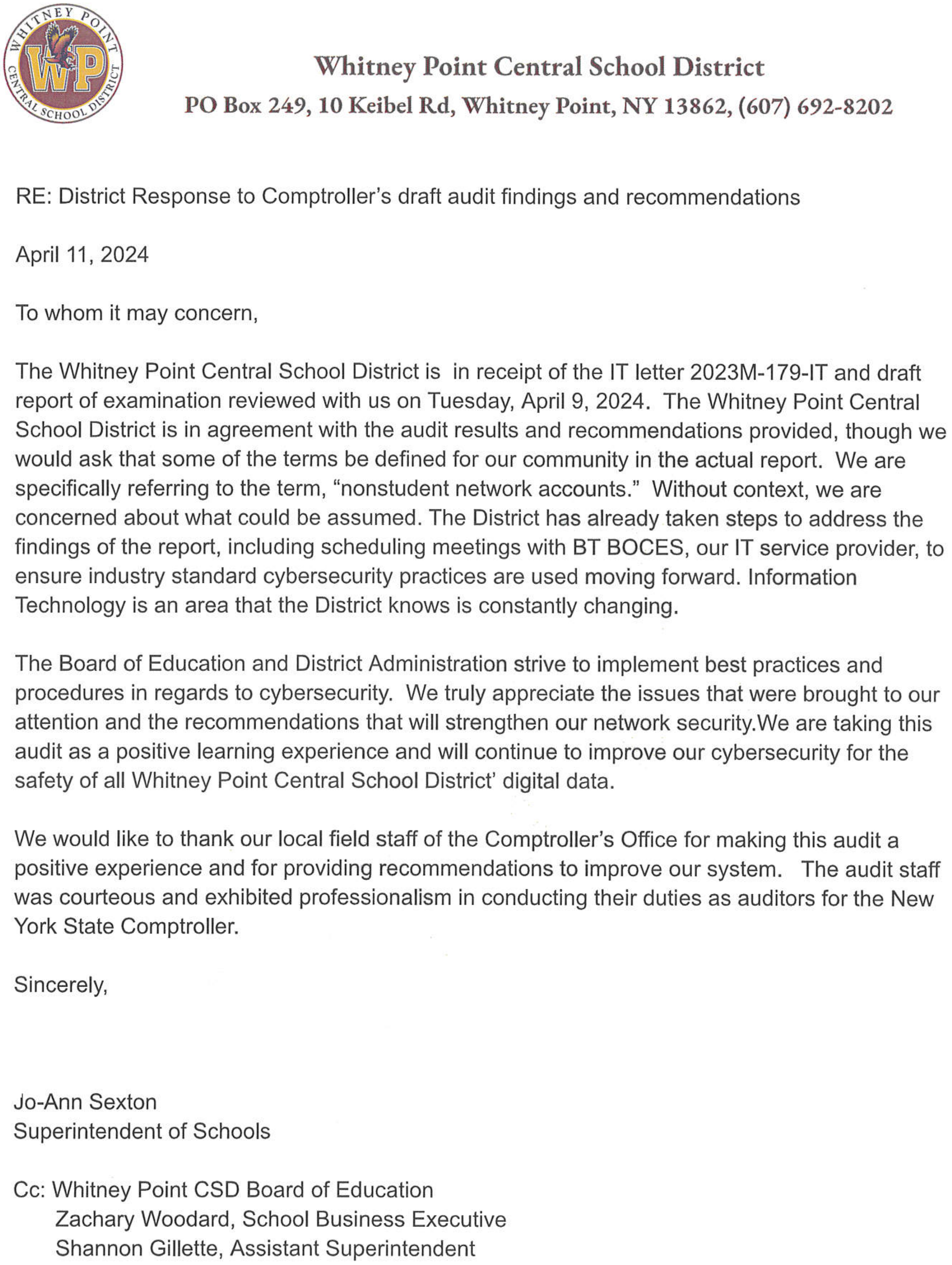
1. Evaluate all enabled nonstudent network user accounts and disable accounts when they are no longer needed.

2. Develop written procedures for granting, modifying and disabling nonstudent user account access to the District's network and periodically reviewing all nonstudent network user accounts, including a timeline for disabling unneeded and unused user accounts added by SCRIC staff.

The Board should:

3. Review and adopt their comprehensive IT contingency plan, update the plan as needed and distribute it to all responsible parties.

Appendix A: Response From District Officials



Whitney Point Central School District
PO Box 249, 10 Keibel Rd, Whitney Point, NY 13862, (607) 692-8202

RE: District Response to Comptroller's draft audit findings and recommendations

April 11, 2024

To whom it may concern,

The Whitney Point Central School District is in receipt of the IT letter 2023M-179-IT and draft report of examination reviewed with us on Tuesday, April 9, 2024. The Whitney Point Central School District is in agreement with the audit results and recommendations provided, though we would ask that some of the terms be defined for our community in the actual report. We are specifically referring to the term, "nonstudent network accounts." Without context, we are concerned about what could be assumed. The District has already taken steps to address the findings of the report, including scheduling meetings with BT BOCES, our IT service provider, to ensure industry standard cybersecurity practices are used moving forward. Information Technology is an area that the District knows is constantly changing.

See Note 1 Page 7

The Board of Education and District Administration strive to implement best practices and procedures in regards to cybersecurity. We truly appreciate the issues that were brought to our attention and the recommendations that will strengthen our network security.We are taking this audit as a positive learning experience and will continue to improve our cybersecurity for the safety of all Whitney Point Central School District' digital data.

We would like to thank our local field staff of the Comptroller's Office for making this audit a positive experience and for providing recommendations to improve our system. The audit staff was courteous and exhibited professionalism in conducting their duties as auditors for the New York State Comptroller.

Sincerely,

Jo-Ann Sexton
Superintendent of Schools

Cc: Whitney Point CSD Board of Education
Zachary Woodard, School Business Executive
Shannon Gillette, Assistant Superintendent

Appendix B: OSC Comment on the District's Response

Note 1

We revised the audit report to define nonstudent network user accounts.

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. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed District officials and SCRIC staff, and reviewed Board meeting minutes and District and SCRIC IT policies and procedures, to gain an understanding of the District's IT operations, including the management of nonstudent network user accounts and determining whether the District had an IT contingency plan.
- We ran a computerized audit script on the District's network on February 24, 2023. We analyzed the reports generated by the script for weaknesses in the District's nonstudent network user account management. We reviewed all 508 enabled nonstudent network user accounts and compared all network account users to current District employee and SCRIC employee lists to identify unused and other possibly unneeded network user accounts.
- We reviewed screenshots and system reports to confirm that periodic backups were conducted and backup file restorations were successful.

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.

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.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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief of Municipal Audits

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins counties