DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-104

Potsdam Central School District

Network User Account Controls and Information Technology Contingency Planning

DECEMBER 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Potsdam Central School District

Audit Objective

Determine whether Potsdam Central School District (District) officials established adequate controls over network user accounts and developed an information technology (IT) contingency plan.

Key Findings

District officials did not establish adequate controls over network user accounts and did not develop a written IT contingency plan. As a result, the District had additional entry points for attackers to access and view personal, private and sensitive information on the network and did not have sufficient documented guidance or plans to follow to resume essential operations if an unexpected IT incident occurred.

In addition to finding sensitive IT control weaknesses that were confidentially communicated to officials, we found that:

- Of the District's 1,909 network user accounts 1,896 network user accounts were granted unneeded administrative permissions.
- 105 network user accounts were unneeded.

Key Recommendations

- Develop written procedures for managing and reviewing network user accounts.
- Develop a comprehensive written IT contingency plan.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The District serves the Towns of Canton, Parishville, Pierrepont, Potsdam and Stockholm in St. Lawrence County.

The District is governed by a nine-member Board of Education (Board) responsible for the management and control of financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible for District administration.

The Assistant Superintendent of Curriculum and Instruction (Assistant Superintendent) oversees the District's IT operations. The St. Lawrence-Lewis Board of Cooperative Educational Services (BOCES) and Northeastern Regional Information Center (NERIC) provide IT services to the District, including two shared network administrators (administrators) and management of the District's network.

Quick Facts	
Student Enrollment	1,213
Employees	334
Network User Accounts	
Student	1,491
Non-Student	418

Audit Period

July 1, 2020 – December 20, 2021

Information Technology

How Should Officials Adequately Control Network User Accounts?

A school district relies on its network for maintaining financial, student and personnel records and Internet access and email, much of which contain personal, private and sensitive information (PPSI).[1] A network user account is used to access a school district's network. Network user accounts are managed centrally by a server and/or domain controller and can be assigned to various security groups. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application.

School district officials are responsible for restricting network user account access to only those resources needed for students to access their learning and employees, officials and third parties to complete their job duties and responsibilities. This helps ensure data and IT assets are protected from unauthorized use and/or modification. A school district should have written policies and procedures for granting, changing and removing user access and permissions to the network.

When unneeded network user accounts exist, the school district has an increased risk that PPSI could be intentionally or unintentionally changed and/or compromised by unauthorized individuals. Officials should disable unnecessary network user accounts when they are no longer needed. To minimize the risk of unauthorized use, access and loss, officials should actively manage network user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. If not properly managed, unnecessary network user accounts may not be detected and disabled timely, and they could be additional entry points for attackers to access and view PPSI on the network.

Service accounts are accounts created to run a particular network or system service or application. Service accounts should be limited in use, as they are not linked to individual users and may have reduced accountability. For example, service accounts may be created and used for automated backup or testing processes, or generic email accounts such as a service help desk account. Officials should limit the use of service accounts, routinely evaluate the need for these accounts and disable those that are not related to a current school district or system need.

A shared account has a username and password that is shared among two or more people. Because shared accounts are not assigned to a single user, officials may have difficulty linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own

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

user account and password to gain access to a network. If shared accounts are needed, officials should have procedures in place to monitor their use to ensure accountability over work performed and data changed or deleted.

Network accounts with administrative permissions can be used to perform activities such as installing software, creating user accounts and changing security settings. Officials must ensure that accounts with administrative permissions are appropriately assigned based on the access needed for each user's role within the school district. Additionally, because these accounts have higher privileges, school districts should consider additional safeguards to restrict access. For example, segregating duties so that user account access is approved by one individual and created, updated, and deleted by a separate, independent individual.

Officials Did Not Adequately Manage Network Administrative Permissions

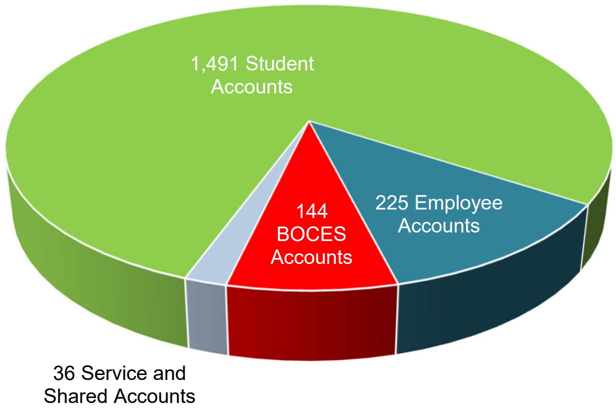
The District does not have written policies or procedures to help prevent user accounts from being granted administrative permissions without authorization. All 1,909 network user accounts had administrative permissions on the District's domain controller.

The District does not have written policies or procedures to help prevent user accounts from being granted administrative permissions without authorization.

The administrators[2] told us that permissions for 13 of these accounts were necessary to administer the network (seven BOCES accounts and six service and shared accounts). The remaining 1,896 network user accounts had unneeded network administrative permissions based on the access needed for each account user's role within the District (Figure 1).

FIGURE 1

Unneeded Network Administrative Permissions by User Account Type



[2] During our audit period, two network administrators were responsible for managing the District's network. One NERIC administrator was there for the entire audit period; the other BOCES administrator began in July 2021.

The administrators told us that while elevating certain permissions for the maintenance group, they inadvertently included all network user accounts in a group that had administrative permissions and were unaware this occurred. The District did not have additional safeguards to prevent this, such as segregating duties so that user account access was approved by one individual and created, updated, and deleted by a separate, independent individual. Consequently, the unneeded permissions were not identified or corrected. After the administrators were made aware of this oversight during our audit, they promptly removed the unneeded administrative permissions for the 1,896 network user accounts.

When users have unneeded administrative permissions to a network, they could make unauthorized changes that may not be detected. In addition, the misuse of administrative permissions is a method used by attackers to compromise or disrupt systems. A user can be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website, or accessing a website programmed to automatically infect the user's computer with malicious software. If the user has administrative permissions, an attacker could use those elevated privileges to cause greater damage than with a lesser-privileged account.

Officials Did Not Adequately Manage All Network User Accounts

The District's Computer Resources and Data Management Policy and Regulation (Policy) requires that the Superintendent, working with the Assistant Superintendent and the Business Manager, establish password and user access procedures. However, the District did not have written procedures for creating, modifying or disabling network user accounts and did not adequately manage all network user accounts. The Assistant Superintendent and administrators told us they have informal procedures for user account management, including annual reviews of all non-student and non-service network user accounts. Annually, all student network accounts are disabled, and new accounts are created for each student. The Superintendent told us that it was an oversight that written network access procedures were not established.

…[T]he District did not have written procedures for creating, modifying or disabling network user accounts and did not adequately manage all network user accounts.

We reviewed all 418 non-student enabled network user accounts (225 employee accounts, 151 BOCES staff and 42 service and shared accounts) to determine whether they were needed. We found 105 user accounts (25 percent) that were not needed. After we brought this to the administrators' attention, they told us they disabled all 105 unneeded network user accounts, as discussed below.

<u>BOCES Accounts</u> – During our review of the 151 BOCES network user accounts, we found 91 accounts (60 percent) that should have been disabled. These accounts were not needed because these BOCES employees began using a BOCES network in August 2020 to perform their job duties and no longer needed a District network user account. The administrators told us that they were aware

of the change, and not disabling these accounts was an oversight. The remaining 60 user accounts were for BOCES employees who needed a District network user account to access certain District applications based on their job duties.

Service and Shared Accounts – During our review of the 42 service and shared network user accounts, we found 12 unneeded service accounts (29 percent) that were not used in over two years. Two of these accounts were not used in over six years. The administrators told us that these service accounts were not included in the annual review of user accounts because their annual review only includes non-student and non-service network user accounts. The review does not include service and shared accounts. As a result, these user accounts were not identified and disabled when they were no longer needed. In addition, the District should have a procedure that triggers account disabling when services are no longer needed.

We also found three accounts that were shared accounts, including two substitute teacher accounts and one guest account. The administrators told us that the two substitute teacher accounts' usernames and passwords are provided to daily substitutes by the building principals to access the District's network. The guest account is mainly used for presentations or meetings. The administrators told us the three shared accounts were necessary. However, the District did not establish procedures to monitor who used the shared accounts and when they were used. The Superintendent told us that it was an oversight that the District did not establish these procedures.

Employee Accounts – When new employees are hired or if an employee network user account modification is necessary, the District Clerk submits a work ticket with requests to add or modify network user accounts. In addition, network user accounts are disabled after the District Clerk submits a work ticket or emails written notification to one of the administrators or a BOCES computer technician. During our review of the 225 employee network user accounts, we found two user accounts assigned to former employees that separated from the District in August 2019 and January 2021. The administrators agreed that the accounts should have been disabled and that it was an oversight.

The unneeded network user accounts are additional entry points into the District's network and, if accessed by an attacker, could 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. 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, such as student medical records or individualized education programs;

- Installing malicious software that could cripple and/or completely shut down the District's network by accessing a service account with administrative permissions;
- Obtaining and publicly releasing PPSI, such as employee and student dates of birth, home addresses and social security numbers, that could be used to facilitate identity theft; and
- Inappropriately accessing and changing District records, such as student grades.

Why Should a District Have a Written IT Contingency Plan?

An IT contingency plan is a school district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of IT operations after an unexpected incident. A written contingency plan should address potential threats to the IT system(s) and be updated as needed. An unexpected incident could include a power outage, software failure caused by a virus or malicious software, equipment destruction, inadvertent employee action or a natural disaster, such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such an event.

The content, length and resources necessary to prepare an IT contingency plan vary depending on the size and sophistication of a school district's computerized operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to help enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Backup policies and procedures are also critical components and help ensure that information is routinely backed up and available in the event of a disruption.

The IT contingency plan can also include, among other items deemed necessary by school officials, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Communication protocols with outside parties,
- Prioritized mission critical processes,
- Technical details concerning how systems and data will be restored,

- Resource requirements necessary to implement the plan,
- Backup methods and storage policies, and
- Details concerning how the plan will be periodically tested.

The District Did Not Have a Comprehensive Written IT Contingency Plan

The Board and District officials did not develop and adopt a comprehensive written IT contingency plan to describe the measures officials should take to respond to potential disruptions and disasters affecting the District's IT environment. Consequently, in the event of a disruption or disaster, such as a ransomware attack, employees have no official guidance to help resume, restore, repair and/or rebuild essential operations in a timely manner.

The Board and District officials did not develop and adopt a comprehensive written IT contingency plan to describe the measures officials should take to respond to potential disruptions and disasters affecting the District's IT environment.

Although the District has detailed backup procedures and technical details concerning how systems and data will be restored, the backup procedures were inadequate because they do not include steps to verify data has been backed up and can be restored when needed. Therefore, there is no assurance the procedures would be sufficient and effective in the event of an emergency.

According to discussions with officials and review of the District's Policy, the Superintendent tasked the Assistant Superintendent with developing the IT contingency plan. The Assistant Superintendent was new to this position in July 2021 and told us he has not had time to develop the IT contingency plan. The Superintendent had not designated anyone to this task prior to the Assistant Superintendent's promotion. However, the Board and Superintendent should have ensured a plan was in place prior to the time of the Assistant Superintendent's promotion, because without a comprehensive written IT contingency plan, there is an increased risk that the District could lose important data and suffer a serious interruption to operations, such as not being able to process paychecks, vendor payments, student grades or State aid claims. This is particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks currently facing school districts.

What Do We Recommend?

The Board should:

1. Require the Superintendent, Assistant Superintendent and Business Manger to create comprehensive written procedures for granting, changing, revoking and reviewing network user access and permissions and ensure the procedures are developed and implemented by District officials.

The Board and District officials should:

2. Develop and adopt a comprehensive written IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

District officials should:

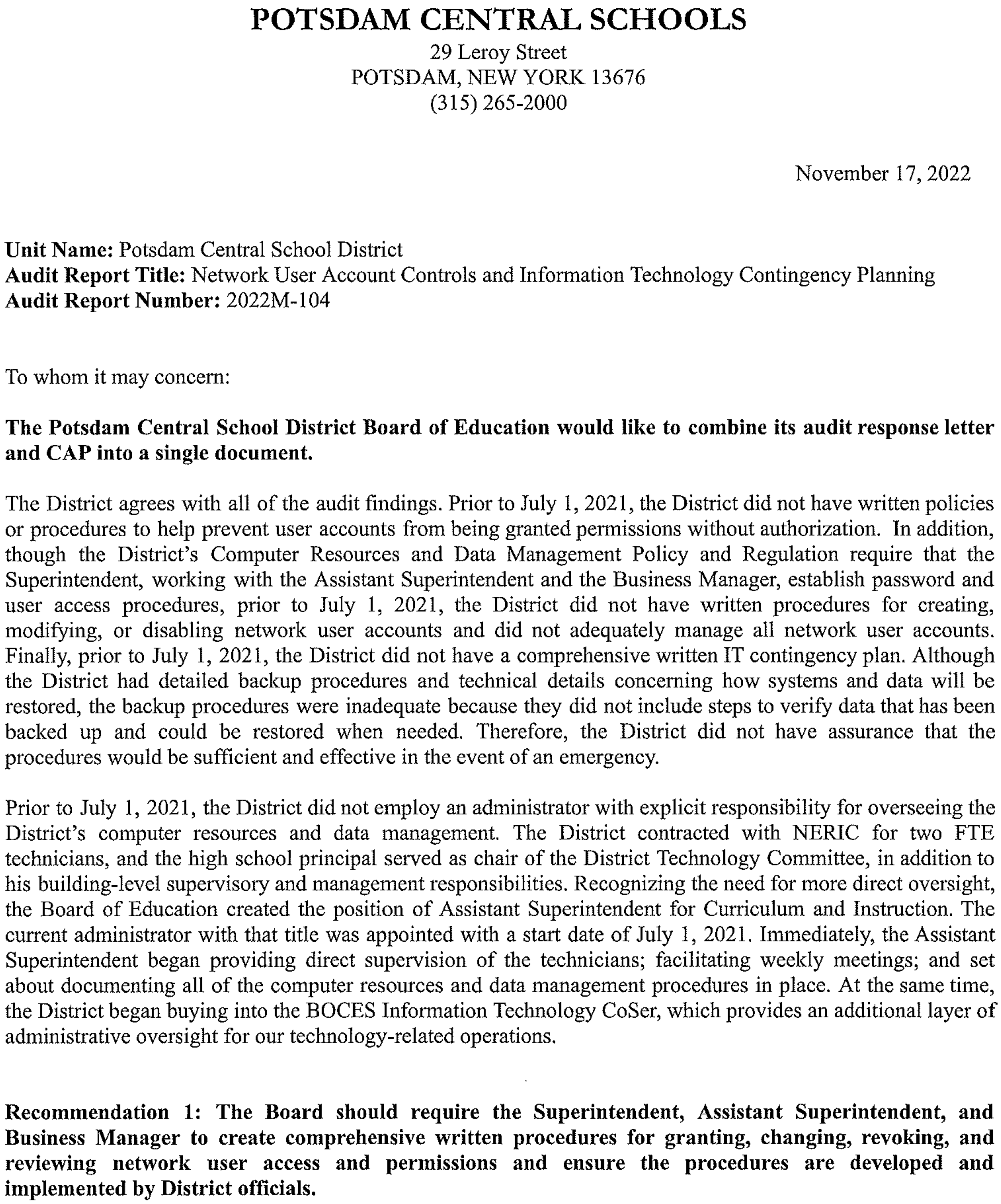
3. Develop comprehensive written procedures for granting, changing, revoking and reviewing network user access and permissions.

4. Assess network user permissions on a regular basis and ensure that network administrative permissions are limited and network user accounts provide only those permissions needed for account users' roles within the District.

5. Evaluate all existing network accounts, disable any deemed unneeded and ensure effective procedures are in place to detect and disable unneeded network user accounts in a timely manner.

6. Restrict the use of shared network user accounts and/or develop procedures to monitor who uses these accounts and when they are used.

Appendix A: Response From District Officials



POTSDAM CENTRAL SCHOOLS

29 Leroy Street
POTSDAM, NEW YORK 13676
(315) 265-2000

November 17, 2022

Unit Name: Potsdam Central School District
Audit Report Title: Network User Account Controls and Information Technology Contingency Planning
Audit Report Number: 2022M-104

To whom it may concern:

The Potsdam Central School District Board of Education would like to combine its audit response letter and CAP into a single document.

The District agrees with all of the audit findings. Prior to July 1, 2021, the District did not have written policies or procedures to help prevent user accounts from being granted permissions without authorization. In addition, though the District's Computer Resources and Data Management Policy and Regulation require that the Superintendent, working with the Assistant Superintendent and the Business Manager, establish password and user access procedures, prior to July 1, 2021, the District did not have written procedures for creating, modifying, or disabling network user accounts and did not adequately manage all network user accounts. Finally, prior to July 1, 2021, the District did not have a comprehensive written IT contingency plan. Although the District had detailed backup procedures and technical details concerning how systems and data will be restored, the backup procedures were inadequate because they did not include steps to verify data that has been backed up and could be restored when needed. Therefore, the District did not have assurance that the procedures would be sufficient and effective in the event of an emergency.

Prior to July 1, 2021, the District did not employ an administrator with explicit responsibility for overseeing the District's computer resources and data management. The District contracted with NERIC for two FTE technicians, and the high school principal served as chair of the District Technology Committee, in addition to his building-level supervisory and management responsibilities. Recognizing the need for more direct oversight, the Board of Education created the position of Assistant Superintendent for Curriculum and Instruction. The current administrator with that title was appointed with a start date of July 1, 2021. Immediately, the Assistant Superintendent began providing direct supervision of the technicians; facilitating weekly meetings; and set about documenting all of the computer resources and data management procedures in place. At the same time, the District began buying into the BOCES Information Technology CoSer, which provides an additional layer of administrative oversight for our technology-related operations.

Recommendation 1: The Board should require the Superintendent, Assistant Superintendent, and Business Manager to create comprehensive written procedures for granting, changing, revoking, and reviewing network user access and permissions and ensure the procedures are developed and implemented by District officials.

Implementation Plan of Action: The Assistant Superintendent, in collaboration with the BOCES and NERIC IT technicians, has created a comprehensive Potsdam Central School District Information Technology Manual. This document includes written procedures for granting, changing, revoking, and reviewing network user access and permissions.
Implementation Date: The Information Technology Manual will be presented to the Board of Education by March 1, 2023. The manual will be reviewed and updated annually, and any recommended changes presented to the Board of Education for their adoption.
Person Responsible for Implementation: Assistant Superintendent for Curriculum and Instruction

Recommendation 2: Develop and adopt a comprehensive written IT contingency plan and ensure it is distributed to all responsible parties, periodically tested, and updated as needed.

Implementation Plan of Action: The Assistant Superintendent, in collaboration with the BOCES and NERIC IT technicians, has created a comprehensive Potsdam Central School District Information Technology Manual. This document includes a written IT contingency plan, which will be distributed to all responsible parties, periodically tested, and updated as needed.
Implementation Date: The Information Technology Manual will be presented to the Board of Education by March 1, 2023. The manual will be reviewed and updated annually, and any recommended changes presented to the Board of Education for their adoption.
Person Responsible for Implementation: Assistant Superintendent for Curriculum and Instruction

Recommendation 3: Develop comprehensive written procedures for granting, changing, revoking and reviewing network user access and permissions.

Implementation Plan of Action: The Assistant Superintendent, in collaboration with the BOCES and NERIC IT technicians, has created a comprehensive Potsdam Central School District Information Technology Manual. This document includes written procedures for granting, changing, revoking, and reviewing network user access and permissions.
Implementation Date: The Information Technology Manual will be presented to the Board of Education by March 1, 2023. The manual will be reviewed and updated annually, and any recommended changes presented to the Board of Education for their adoption.
Person Responsible for Implementation: Assistant Superintendent for Curriculum and Instruction

Recommendation 4: Assess network user permissions on a regular basis and ensure that network administrative permissions are limited, and network user accounts provide only those permissions needed for account users' roles within the District.

Implementation Plan of Action: Using a script provided by staff from the Office of the Comptroller, a schedule was created so that all servers are scanned monthly to ensure that network administrative permissions are limited, and network user accounts provide only those permissions needed for account users' roles within the District.
Implementation Date: The schedule was implemented November 1st, 2022.
Person Responsible for Implementation: NERIC Network Administrator

Recommendation 5: Evaluate all existing network accounts, disable any deemed unneeded and ensure effective procedures are in place to detect and disable unneeded network user accounts in a timely manner.

Implementation Plan of Action: All existing network accounts have been evaluated, and any accounts deemed unneeded have been disabled. Using a script provided by staff from the Office of the Comptroller, a schedule was created so that all servers are scanned monthly to ensure that network administrative permissions are limited, and network user accounts provide only those permissions needed for account users' roles within the District.
Implementation Date: The schedule was implemented November 1st, 2022.
Person Responsible for Implementation: NERIC Network Administrator

Recommendation 6: Restrict the use of shared network user accounts and/or develop procedures to monitor who uses these accounts and when they are used.

Implementation Plan of Action: As of November 1st, 2022, the number of shared network accounts were reduced and procedures were implemented to ascertain who uses the remaining shared accounts and monitor them when in use. As of December 1st, when an individual is given access to a shared account, the date(s) of use will be logged and maintained for reference.
Implementation Date: This procedure will be implemented December 1st, 2022.
Person Responsible for Implementation: Building-level Principals and Secretaries

The Potsdam Central School District recognizes the importance of establishing adequate controls over network user accounts and developing an information technology (IT) contingency plan. In establishing an administrative position in the District with responsibility for computer resources and data management, the Board of Education had already taken an important first step in ensuring adequate oversight is provided. Work on the Information Technology Manual was already underway at the time this audit took place. The recommendations provided were helpful as we implemented procedures for managing and reviewing network user accounts. The steps we have taken since July 1, 2021, have reduced the likelihood attackers would be able to access and view personal, private, and sensitive information on the network. The written guidance we now have in place will provide plans for us to follow to resume essential operations if an unexpected IT incident occurred.

Sincerely,

Joann Chambers
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 interviewed District officials, BOCES and NERIC staff, and reviewed the District's IT policies and procedures to gain an understanding of the IT environment, specifically those related to network user account controls, and to determine whether the District had an adequate IT contingency plan.
- We examined all network user accounts and security settings on the District's domain controller, the server in the network used to help control and manage all computer and user accounts, as of July 15, 2021 using a computerized audit script. We analyzed the generated reports to review the non-student user accounts and compared them to current employee lists to identify inactive and possibly unneeded enabled network user accounts. We also reviewed network user accounts assigned to BOCES staff and identified any shared and service accounts and discussed the necessity of the network user accounts we reviewed with District officials and third parties.
- We reviewed all network user accounts with administrative permissions and discussed them with District officials and third parties to determine whether permissions were appropriate and needed.

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 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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief of Municipal Audits

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller