DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-125

Hunter-Tannersville Central School District

Network User Accounts and Information Technology Contingency Planning

NOVEMBER 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Hunter-Tannersville Central School District

Audit Objective

Determine whether Hunter-Tannersville Central School District (District) officials adequately managed and monitored nonstudent network user accounts and developed a comprehensive written information technology (IT) contingency plan.

Key Findings

District officials did not adequately manage or monitor nonstudent network user accounts or develop a written IT contingency plan.

In addition to sensitive IT control weaknesses that were communicated confidentially to officials, we found that officials did not:

- Disable 31 unneeded network user accounts (of the 225 enabled nonstudent accounts) including, but not limited to, accounts for former employees and substitute teachers that were never employed by the District. As a result, the District's risk of unauthorized network access is increased.
- Develop and adopt a comprehensive written IT contingency plan or store back-up data off site.

Key Recommendations

- Develop and communicate comprehensive written procedures for managing and monitoring nonstudent network user account access.
- Develop and adopt a comprehensive written IT contingency plan and store back-ups off site.

District officials agreed with our recommendations and indicated that they are implementing corrective action.

Background

The District serves the Towns of Halcott, Hunter, Jewett, Lexington and Prattsville in Greene County.

The District is governed by an elected five-member Board of Education (Board), responsible for managing and controlling financial and educational affairs.

The Superintendent of Schools (Superintendent) is appointed by the Board and is chief executive officer responsible for day-to-day management, under the Board's direction.

The District's Director of Technology (Director) is responsible for managing and monitoring the District's IT operations including nonstudent network user accounts and IT contingency planning, and reports to the Superintendent.

Quick Facts	
Employees	140
Enabled Network User Accounts	
Student	301
Nonstudent	225

Audit Period

July 1, 2020 – July 27, 2021

Network User Accounts and IT Contingency Planning

The District's IT system and data are valuable resources. The District relies on its IT assets for maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI)[1] and is accessed through network user accounts, email and Internet access. If the IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate and repair. Proactively anticipating and planning for IT disruptions will prepare District personnel for the actions they must take in the event of an incident. While effective controls, such as adequately managed and secured network user accounts, will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

These network user accounts are potential entry points for attackers. …

How Should District Officials Manage and Monitor Nonstudent Network User Accounts?

Nonstudent network user accounts provide access to network resources such as shared folders and email, and should be properly managed and monitored to minimize the risk of misuse. These network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and then view, modify and/or delete PPSI on the network. A district should have comprehensive written procedures for managing and monitoring nonstudent network user accounts. These procedures should be communicated to and enforced by responsible officials and employees (e.g., the Director and District office staff). Officials should disable unnecessary accounts as soon as they are no longer needed. In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed.

Shared and service network user accounts should be limited in use 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 (e.g., substitute teachers and contracted vendors). Service user accounts are accounts created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems). Officials should limit the use of shared and service accounts and also routinely evaluate the need for the accounts and disable those that are not related to a current district or system need. If shared and service accounts are needed, officials should have procedures in place to monitor who uses the accounts and when and how they are used. This helps ensure accountability over work performed and data changed or deleted.

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general.

The Director Did Not Adequately Manage or Monitor Nonstudent Network User Accounts

The Director did not adequately manage or monitor nonstudent network user accounts or perform periodic reviews of all enabled District nonstudent network user accounts to identify any unnecessary network user accounts. We examined the 225 enabled nonstudent network user accounts to determine whether any were unneeded and found 31 unneeded accounts. Specifically, there were:

- 11 network user accounts were for former employees whose accounts were not disabled. For example, the user account for a former employee who left District employment in June 2019 was not disabled.
- 11 unneeded shared network accounts that had been used mostly by elementary school teachers and librarians. According to the Director, shared accounts were created for each elementary school classroom because elementary school students do not get their own network accounts.
- Six unique network user accounts expected to be used by substitute teachers that never were employed by the district. Although these accounts were created between September 2019 and December 2020, they were never used and were not disabled on the network.
- Three unneeded service accounts used for testing network permissions, accessing a former student management system, and email archiving.

We attribute these findings, in part, to the officials not developing comprehensive written procedures for managing or monitoring nonstudent network user accounts. Subsequent to audit fieldwork, District officials developed an exit checklist that identified the Director as responsible for removing network accounts upon separation from the District to help ensure unnecessary accounts were disabled timely. Despite the lack of comprehensive written procedures, monitoring activities, such as conducting a periodic review of all enabled network user accounts, could have helped detect unnecessary network user accounts that were not disabled.

Leaving former employee and unneeded shared and service user accounts enabled on the network increases the risk of unauthorized access because any account on a network is a potential entry point for attackers. Of particular risk are enabled network user accounts for former employees and substitute teachers, as these could potentially be used by those individuals or others for malicious activities. Because some of these unneeded network user accounts had access to student data, an attacker may be able to leverage student data for personal gain (e.g., selling student data or identity theft) if they were to gain unauthorized access to the network.

Why Should District Officials Adopt an IT Contingency Plan?

To help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster, a board and district officials should develop and adopt a comprehensive written IT contingency plan. An IT contingency plan is a district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT disruption or disaster. The plan should address the potential for sudden, unplanned disruptions (e.g., system failure caused by an inadvertent employee action, power outage, ransomware or other type of malware infection or a natural disaster such as a flood or fire) that could compromise the network and the availability or integrity of the school district's IT system and data, including PPSI contained therein.

Typically, IT contingency planning involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to maintain or quickly resume, restore, repair and/or rebuild operations. It should also reference how the school district should back up its computer systems and data. Backup data should be stored at a secure offsite location, maintained off-network, encrypted and routinely tested to ensure its integrity. The plan should also be periodically tested, updated as needed, and distributed to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes, such as statutory changes.

…[O]fficials have no District-specific guidelines to help minimize or prevent the loss of equipment and data. …

The Board and District Officials Did Not Adopt an IT Contingency Plan

The Board and District officials did not develop and adopt a written IT contingency plan. Although the Technology Department performs daily backups of District servers, backup restoration is not periodically tested to ensure the backup process is running correctly and backup data maintains its integrity and would be available when needed. Additionally, backups are stored securely on-site rather than an off-site location. Consequently, in the event of an unplanned IT disruption or disaster, officials have no District-specific guidelines to help minimize or prevent the loss of equipment and data, or assurance that data, including other critical data not stored on District servers, can be recovered appropriately to resume operations. Officials also did not have clear guidance identifying roles of key individuals and necessary precautions to maintain or quickly resume, restore, repair and/or rebuild operations.

According to the Superintendent, the Board and District officials did not develop and adopt an IT contingency plan because it was not required. Although an IT contingency plan is not a statutory requirement, it is a longstanding best practice and essential tool for preparing school personnel for the actions they must take in the event of an unexpected IT disruption.

School districts heavily rely on IT to keep educational systems functioning while also helping to keep PPSI protected and secure. Without a written IT contingency plan in place that is distributed to all responsible parties and periodically tested for efficacy, District officials have less assurance that employees will react quickly and effectively to maintain business continuity. In addition, officials cannot ensure the recovery of necessary data to continue its computerized operations. As a result, the District could lose important data and suffer a serious interruption to operations that depend on its computerized environment, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims.

What Do We Recommend?

The Director should:

1. Develop and communicate comprehensive written procedures for managing and monitoring nonstudent network user account access that ensure network user accounts are disabled once they are no longer needed.

2. Disable network user accounts of former employees and other users as soon as they are no longer needed and maintain and periodically evaluate a list of authorized nonstudent network user accounts.

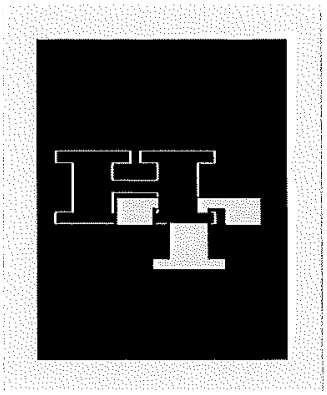
3. Ensure all network users have and use their own unique network user accounts to access the District's network or develop procedures to monitor shared and service accounts as to who uses the accounts and when and how they are used.

The Board and District officials should:

4. Develop and adopt a comprehensive written IT contingency plan and ensure it is periodically tested, updated and distributed to all key officials.

5. Store backup data at a secure off-site location, ensuring the data is maintained off-network, encrypted and routinely tested to ensure its integrity.

Appendix A: Response From District Officials



Hunter-Tannersville Central School District
Office of the Superintendent
6094 Main Street, P.O. Box 1018, Tannersville, N.Y. 12485
518-589-5400 Ext. 1000 www.htcschools.org

October 28, 2022

Office of the State Comptroller
Division of Local Government and School Accountability
Chief Examiner, Dara Disko-McCagg
Newburgh Regional Office
33 Airport Center Driver, Suite 103
New Windsor, New York 12553

Re: Hunter-Tannersville CSD
Network User Accounts & Information Technology Contingency Planning
Audit Period - July 1, 2020 - July 27, 2021
Audit Report Number - 2022M-125

Dear Chief Examiner Disko-McCagg,

Hunter-Tannersville CSD has received the Draft Audit Report titled Network User Accounts & Information Technology Contingency Planning.

The Board of Education, District Administration, and the Director of Technology appreciate the thorough work and recommendations provided by the Office of the State Comptrollers. Recognizing that technology continues to demonstrate rapid growth and expansion into all school district functions is essential. Thus creating more vulnerabilities for school districts. The OSC audit team has provided the district with strategic recommendations to support our ability to mitigate cyber-attacks.

Before the audit began, Hunter-Tannersville recognized the urgency to improve our IT controls to protect district assets and confidential data. We began collaborating with the Capital Region BOCES Cyber and Vendor Risk Management service designed to identify, mitigate, and manage cyber risks. For several months now, HTC has been working with Capital Region BOCES, who are providing the following services to the district:

- **IT Risk Assessment** — Analysis is centered on publicly-accessible systems that can be observed from the internet.
- **Board IT Policy Review** — We will review Board IT policies against current federal and state requirements and will provide recommendations for each policy and where deemed appropriate.
- **General Liability and Cyber Insurance Review** — At the organization's discretion, we will develop and facilitate the process for an Insurance RFP and/or a review of your current cyber liability insurance.
- **Compliance Analysis with Industry, Federal and State Standards** — Using a number of online assessment tools, a gap analysis will be conducted, and an action plan created to assist the organization in increasing their level of compliance. Project Management support will be provided throughout the agreement to implement the action plan.
- **Training and Advisement, Including Awareness and Incident Response Training** — We will provide training materials and guidance related to awareness and incident response training. The training and guidance provide staff with the knowledge, skills and resources regarding data, cyber security, vendor risk management and responding to a cyber security incident.
- **Vendor Risk Vetting** — An assessment and recommendation will be conducted on vendors which the organization would like to engage with. The assessment will be based on information provided by the vendor regarding their compliance with New York State Education Law 2-d and NIST CSF compliance.
- **Facilitate Data Privacy Agreements**

The correction action plan (CAP), represented in the table below, outlines our agreement with OSC and our specific improvement plan. We believe that our CAP and the additional Cyber Risk and Vendor Management service support will provide the district with a robust plan to mitigate threats.

Recommendations	Agree or Disagree	Intended Actions	Person Responsible
Recommendation #1: Develop and communicate comprehensive written procedures for managing and monitoring nonstudent network user account access that ensure network	Agree	**District Response:** The unneeded accounts have been removed. The district office and IT Director have worked on the processes in place for notifying each other of staff changes. They have put checklists together for when an employee enters or leaves the district. A plan is also	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team

user accounts are disabled once they are no longer needed.		being formulated for conducting regular reviews of network accounts annually. The district is currently working with the NERIC Cybersecurity Risk service on properly documenting IT procedures and policies.	
Recommendation #2: Disable network user accounts of former employees and other users as soon as they are no longer needed and maintain and periodically evaluate a list of authorized nonstudent network user accounts.	Agree	**District Response:** The unneeded accounts have been removed. The district office and IT Director have worked on the processes in place for notifying each other of staff changes. They have put checklists together for when an employee enters or leaves the district. A plan is also being formulated for conducting regular reviews of network accounts annually. The district is currently working with the NERIC Cybersecurity Risk service on properly documenting IT procedures and policies.	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team
Recommendation #3 Ensure all network users have and use their own unique network user accounts to access the District's network or develop procedures to monitor shared and service accounts as to who uses the accounts and when and how they are used.	Agree	**District Response:** The majority of staff and students have their own network accounts. For the grade levels where there are class accounts a process is being documented for monitoring them.	IT Director

Recommendation #4: Develop and adopt a comprehensive written IT contingency plan and ensure it is periodically tested, updated and distributed to all key officials.	Agree	**District Response:** The district is also working with the NERIC Cybersecurity Risk service to improve on the district's IT contingency plan.	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team
Recommendation #5 Store backup data at a secure off-site location, ensuring the data is maintained off-network, encrypted and routinely tested to ensure its integrity.	Agree	**District Response:** The district is also working with the NERIC Cybersecurity Risk service to improve on the district's back strategy	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team

Bobbi Schmitt
Board of Education President

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 District officials to gain an understanding of internal controls over managing and monitoring nonstudent network user accounts and IT contingency planning.
- We ran a computerized audit script on the District's network on July 27, 2021. We then analyzed the data produced to assess nonstudent network user accounts. We excluded student network user accounts, as these accounts had more restricted access and are considered lower risk for potential access to computerized data containing PPSI. We reviewed the remaining 225 nonstudent network user accounts and compared these accounts to the active employee list to identify inactive and unused accounts and discussed these accounts with District officials to determine if the accounts were needed or should have been disabled.
- We used our professional judgment to select a sample of two computers from the District's 760 computers and laptops. We selected computers of users who had access to PPSI and financial software because if this information (e.g., social security numbers and bank account information) were compromised it could negatively impact District operations and employees. We reviewed web history reports from these computers to evaluate whether Internet users were following the computer user's policy.

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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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