New York State Comptroller
THOMAS P. DiNAPOLI

Garrison Union Free School District

Information Technology

2023M-127 | January 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Garrison Union Free School District

Audit Objective

Determine whether Garrison Union Free School District (District) officials secured the District's network user accounts, established physical controls and maintained inventory records for information technology (IT) equipment, and developed an IT contingency plan.

Key Findings

District officials did not adequately secure the District's network user accounts, establish physical controls, maintain complete and accurate inventory records for IT equipment or develop an IT contingency plan. In addition to sensitive IT control weaknesses that we communicated confidentially to District officials, we found:

- District staff did not have sufficient documented guidance or plans to implement following an unexpected IT disruption or disaster. As a result, District officials have an increased risk they may not recover data and resume essential operations in a timely manner.
- 40 of the 115 enabled nonstudent network user accounts (35 percent) were no longer needed. Unneeded user accounts could be used to inappropriately access and view personal, private and sensitive information (PPSI) or disable the network.
- 10 IT assets, including nine laptops and one printer, were not properly recorded in the District's inventory listing.

Key Recommendations

- Develop written procedures for managing network user account access that includes disabling unnecessary network user accounts and periodically reviewing user access.
- Maintain complete, accurate and up-to-date inventory records.
- Develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

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

Background

The District serves the Town of Philipstown in Putnam County and is governed by an elected seven-member Board of Education (Board) responsible for the management of the District.

The Superintendent of Schools (Superintendent), who serves at the Board's discretion, implements District policies and is the chief executive officer. The Superintendent, with their designee, is responsible for securing the District's network.

The School Business Administrator (SBA) is responsible for the District's IT inventory records. The IT Director is responsible for overseeing the IT infrastructure and the District's contracted third-party IT vendor. The current IT Director started in September 2022.

Quick Facts	
Enabled Nonstudent Network User Accounts Reviewed	115
Amount Paid to IT Vendor During Audit Period	$65,146
Approved 2023-24 IT Infrastructure Appropriations	$56,714

Audit Period

July 1, 2021 – February 2, 2023

Information Technology

How Should District Officials Secure Nonstudent Network User Accounts?

Network user accounts provide access to network resources and data needed by employees to complete job duties and other work-related responsibilities. School district (district) officials should secure all network user accounts, including nonstudent network user accounts (e.g., staff accounts, shared and service accounts, third party vendor accounts). District officials should actively manage network user accounts, including their creation, use and dormancy, to ensure they are appropriate and authorized. User accounts that are no longer needed should be disabled immediately. District officials should establish written procedures to help guide network and system administrators in properly granting, modifying and disabling user account access to district networks. These procedures should require district officials to periodically review enabled user accounts to ensure they are appropriate and authorized.

District Officials Did Not Adequately Secure Nonstudent Network User Accounts

The Superintendent and IT Director did not adequately secure nonstudent network user accounts. We reviewed all 115 enabled nonstudent network user accounts on the District's network, including their creation, use and dormancy, to determine whether they were necessary. We identified 40 enabled nonstudent network user accounts (35 percent) that were no longer necessary, as follows:

- 17 enabled nonstudent network user accounts were assigned to former employees, substitute teachers and authorized contractors. The SBA said that 10 user accounts were assigned to former contractors, and that their contracts expired and they were no longer associated with the District. The IT Director confirmed that the remaining seven enabled nonstudent network user accounts were assigned to former employees and substitute teachers that should have been disabled. He said that the previous IT Director did not know how to properly add or remove users from the network and requested support from the IT vendor. Additionally, 14 of these user accounts were never used to log into the network since their creation date, the oldest being an account assigned to a communication consultant in August 2020. Of the remaining three accounts, the oldest had a last logon date in November 2020.
- 23 enabled nonstudent network user accounts were unnecessary shared and service accounts. The IT Director indicated that these accounts were no longer needed for District purposes and would remove them immediately. The two oldest accounts have not been used since June 2016 and October 2017.

The District does not have written procedures to help guide the network and system administrators in properly granting, modifying and disabling user account access to the District's network. The IT Director stated that the previous IT Director emailed the IT vendor to add, remove or modify user access to the network; however, this procedure was not always followed. Since September 2022, District officials established informal procedures to add, remove and modify user access. However, the IT Director did not adequately review all user accounts since starting his position. The IT Director said he intended to review network user accounts over the summer after the 2022-23 school year ended.

Unneeded network user accounts are additional entry points into a network and, if accessed by attackers, could be used to inappropriately access and view PPSI[1] accessible by those accounts, such as special education student data or employee payroll data, and potentially compromise IT resources.

How Should District Officials Maintain IT Inventory Records and Establish Physical Controls for IT Equipment?

District officials should maintain detailed, up-to-date inventory records for all IT equipment. The information maintained for each piece of IT equipment should include a description of the item, including the make, model and serial number; the name of the employee or authorized individual to whom the equipment is assigned; the physical location of the asset; and the relevant purchase or lease information, including the acquisition date.

To further protect these assets, district officials should provide strong physical controls to prevent damage or theft. Such controls that should be implemented include storing portable assets in locked cabinets, closets, rooms or bins that are only accessible by authorized individuals. IT equipment critical to network operations, including servers and switches, should be protected in locked rooms with environmental controls (e.g., smoke detectors, fire alarms, extinguishers and temperature controls). IT equipment should be stored to protect it from water damage, and have an uninterruptible power supply. Furthermore, this equipment should have additional protections, such as a locked server rack cabinet, to ensure only authorized individuals have access to prevent intentional or unintentional harm.

District Officials Did Not Properly Maintain IT Inventory Records and Establish Physical Controls for IT Equipment

After performing a walkthrough of the District's school building and comparing the IT inventory listing to physical assets, we determined that District officials did

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

not establish proper physical controls for IT equipment and maintain complete inventory records.

The IT Director showed the audit team how the power over ethernet injectors,[2] switches and wiring was installed in locations easily accessible to all employees. For example, IT equipment was installed in a room that was also a janitorial closet with plumbing and had no environmental controls, meaning the equipment had a higher risk of being damaged. The IT Director said the District planned on updating the equipment and where it is installed in the summer of 2023. If these high risks are not addressed, at least half the school building will lose Internet capabilities if the equipment is damaged.

Additionally, we determined that 10 (50 percent) of the 20 IT assets sampled[3] were not recorded in the District's IT inventory listing, including nine laptops and one printer. The SBA was unaware that the laptops and printer were missing from the IT inventory listing until we inquired during our testing. The SBA said that the District purchased the nine laptops in 2020 to accommodate remote learning for all the students. Once the laptops arrived, they were subsequently tagged but incorrectly recorded in the inventory listing under one tag number. With respect to the printer, the SBA was unable to determine the source of the printer or why it was not recorded. Because District officials did not adequately review the IT inventory listing, this could have led to an undetected loss of assets. The SBA indicated that the District would update the inventory listing to ensure all IT assets, including the laptops and printer, are recorded properly.

The SBA and IT Director did not properly secure or record IT equipment in their inventory listing, resulting in an increased risk of damage, theft or loss of IT assets. In addition, because assets were not recorded in the inventory listing, the District may not have been reimbursed by insurance companies if assets were lost or damaged.

Why Should the Board and District Officials Develop and 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, the board and district officials should develop and adopt a comprehensive written IT contingency plan. These events can 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 involves analyzing business processes and continuity needs, identifying roles

2 Equipment used to improve network capabilities by improving power to the ethernet cable
3 Refer to Appendix B for information on our sampling methodology.

of key individuals and necessary precautions to recover data and quickly resume operations in the event of an unplanned disruption. Additionally, IT contingency plans should include data backup procedures, such as ensuring backups are stored off-site and off-network, and requiring IT staff to periodically test backups to ensure they will function as expected. District officials should periodically test and update the plan, as needed, to help ensure officials understand their roles and responsibilities during and after a disruptive event. Testing and updating IT contingency plans are particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks. These plans should be distributed 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 Board and District Officials Did Not Develop and Adopt an IT Contingency Plan

The Board and District officials did not develop and adopt an IT contingency plan to document and inform staff how they should respond to unplanned disruptions and disasters that affect the District's IT environment, and procedures for backing up data. The IT Director said that prior to him joining the District in September 2022, IT contingency plans were not written or being developed. This meant that in the event of a disaster or disruption (including ransomware attack or other unplanned events), District staff did not have sufficient documented guidance or plans to follow to recover data and resume essential operations in a timely manner. This also increased potential damage and recovery costs.

The Board adopted a policy in August 2022 stating that the Superintendent and/or their designee will develop an IT contingency plan to help minimize damage caused by disasters or unplanned events. However, the IT contingency plan was not fully developed during our audit period. The IT Director stated that the plan would be in place prior to the beginning of the 2023-24 school year. Without a fully developed and implemented IT contingency plan, the District had an increased risk that it could suffer a serious interruption to operations because the District's inability to communicate during a disruption or disaster could affect the timely processing of its business functions.

What Do We Recommend?

The Board should:

1. Continue working with District officials to update physical controls relating to IT infrastructure from falling behind best practices.

The SBA should:

2. Maintain complete, accurate and up-to-date inventory records.

The Superintendent and IT Director should:

3. Develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

4. Develop written procedures on adding, removing and modifying user access rights.

Appendix A: Response From District Officials

Garrison
Union Free School District

Carl L. Albano, Interim Superintendent
1100 Route 9D P.O. Box 193
Garrison, NY 10524

Tel: (845) 424-3689 Ext. 551
calbano@gufs.org
www.gufs.org

December 22, 2023

State of New York
Office of the State Comptroller
110 State Street
Albany, NY 12236

Subject: Response to New York State Comptroller's Report of Examination (Report 2023M-127)

Dear Ms. Disko-McCagg,

I am writing to formally address the New York State Comptroller's Report of Examination for the Garrison Union Free School District (Report 2023M-127). I sincerely appreciate the dedicated effort you and your associates invested in evaluating our technology procedures, protocols, and best practices covering the period from July 1, 2021, to Feb 2, 2023. The professionalism and courtesy demonstrated by your office staff during their interactions with District personnel did not go unnoticed. Additionally, I value the report's comments, suggestions, and recommendations, and we will carefully consider them.

This response will center on the three recommendations outlined in the report, particularly those discussed during our December 12, 2023 exit interview. It will also serve as a foundation for formulating the District's Corrective Action Plan (CAP).

Comptroller's Recommendation Number One:
Develop written procedures for managing network user account access that include disabling unnecessary network user accounts and periodically reviewing user access.

District Response:
The District has revamped its hiring procedures and incorporated them into an improved handbook. This change includes a refined set of processes for assigning user accounts, a collaboration involving the District Clerk, the Director of Innovation and Learning, and the Principal of Garrison Schools. The process is nearly automated in cases involving students due to the District's transition to online registration. Continuous refinement of this process will occur to address emerging use cases.

Comptroller's Recommendation Number Two:
Maintain complete, accurate, and up-to-date inventory records.

District Response: The District maintains highly accurate records, acknowledging that minor discrepancies may occur with the extensive use of hundreds of devices. Efforts will persist to refine the process, ensuring strong collaboration between the business office and the Director of Innovation and Learning.

Comptroller's Recommendation Number Three:
Develop and adopt a comprehensive written IT contingency plan, update the plan as needed, and distribute it to all responsible parties.

District Response:
During the summer of 2023, the District transitioned to an integrator capable of providing multifaceted support. Electronic files were relocated to their site, which boasts a "twin site" situated across the Hudson River, minimizing the risk of both locations being affected by any disaster. Collaborative efforts with the integrator are ongoing to comprehend their processes and data-safeguarding measures. A comprehensive contingency plan is slated for completion before the conclusion of the 2023-2024 school year.

In conclusion, we appreciate the opportunity to respond to the audit findings, underscoring our commitment to IT system security. The District is dedicated to continually improving its systems, procedures, and protocols. If you have any inquiries regarding this submission, please feel free to contact me. Once this response is accepted, we will promptly prepare the Corrective Action Plan (CAP) with the requisite specificity.

Sincerely,

Carl L. Albano
Interim Superintendent
Garrison Union Free School District

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. 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 reviewed the District's IT policies and procedures and interviewed the Superintendent, SBA and IT Director to gain an understanding of the IT environment and internal controls.
- We reviewed the District's inventory policies and procedures and interviewed the SBA and Treasurer to gain an understanding of the IT inventory environment and internal controls over District IT assets.
- We ran computerized scripts on February 1, 2023 and February 2, 2023 to identify all enabled network user accounts. We excluded all network user accounts associated with students from our audit testing. We compared all remaining 115 enabled nonstudent network user accounts to the active employee list to identify potentially unneeded accounts. We followed up with the SBA and IT Director to determine whether the accounts were needed or should have been disabled.
- We conducted a walkthrough of the District's school building and used our professional judgment to sample 20 portable IT assets. We observed and recorded their tag number, make, model and serial number. We compared the assets to the District's inventory listing to verify whether the asset was properly recorded with the tag number, make, model and serial number.
- We performed a walkthrough of the District's school building with the SBA and IT Director and observed the physical controls for IT assets.

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.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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief of Municipal Audits

33 Airport Center Drive, Suite 102 • 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