DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-135

Nanuet Union Free School District

Network User Accounts and Information Technology Contingency Plan

DECEMBER 2022

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

Contents

Report Highlights

Nanuet Union Free School District

Audit Objective

Determine whether Nanuet Union Free School District (District) officials ensured network user accounts were needed and whether officials adopted an adequate Information Technology (IT) contingency plan.

Key Findings

District officials did not ensure network user accounts were needed, and did not adopt an adequate IT contingency plan. In addition to sensitive IT control weaknesses that we communicated confidentially to officials, we found that officials did not develop:

- Written procedures to identify and disable unnecessary network user accounts. As a result, we identified 18 generic accounts that should have been disabled.
- An adequate comprehensive IT contingency plan to minimize the risk of data loss or prevent a serious interruption of services.

Key Recommendations

- Develop written procedures for managing network user account access.
- Develop and adopt a comprehensive IT contingency plan and communicate it to appropriate officials and employees.

District officials generally agreed with our findings and indicated they plan to initiate corrective action.

Background

The District serves the Town of Clarkstown in Rockland County.

The District is governed by an elected seven-member Board of Education (Board) that is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent is the chief executive officer and is responsible, along with other administrative staff, for the day-to-day management under the Board's direction.

The District's Information Technology Director (IT Director) is responsible for overseeing the acquisition and use of District computer resources. The District contracted with the Lower Hudson Regional Information Center (LHRIC) for IT infrastructure support and the operation of a service desk.

Quick Facts	
Students 2020-21	2,223
Employees	387
Network User Accounts	
Student	**2,034**
Nonstudent	**443**
Generic	**77**
Total	**2,554**

Audit Period

July 1, 2020 – November 9, 2021

Network User Accounts and IT Contingency Plan

How Should School District Officials Ensure that Network User Accounts Are Needed?

A school district's IT system and data are valuable resources. A school district relies on its network and IT assets for maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI)[1] and are accessed through network user accounts, email and Internet access. If the network or IT assets are compromised or disrupted, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and/or rebuild. While effective controls, such as adequately configured and secured network user accounts, will not guarantee the network or IT assets' safety, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized access and misuse. Therefore, school districts should have written procedures for granting, changing and disabling network user accounts. These procedures should establish who has the authority to grant or change user permissions.

School district officials should disable unneeded accounts as soon as there is no longer a need for them. In addition, to minimize the risk of unauthorized access, school district officials should regularly review enabled network user accounts to ensure they are still needed.

Generic user accounts may be needed for certain network services or applications to run properly. However, they should be limited in use because they are not linked to individual users and, therefore, may have reduced accountability. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service help desk account. School district officials should limit the use of generic user accounts, routinely evaluate the need for the accounts, and disable those that are not related to a current school district or system need.

Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized access and misuse.

District Officials Did Not Ensure That Generic Network User Accounts Were Needed

We reviewed all 2,554 enabled network user accounts to determine whether they were still needed. We found that, other than a minor exception which we discussed with District officials, all 2,477 enabled nongeneric accounts identified

[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, customers, third-parties or other individual or entities.

were needed. However, 18 of the 77 generic network user accounts were unneeded and were not disabled on the network.

Although the District has a process to disable unneeded network user accounts for students, employees and contractors, there are no procedures in place to specifically review generic accounts. The IT Director said that the 18 unneeded accounts identified were set up for specific work, and she was not aware that the unneeded accounts were not disabled on the network when the work was completed.

Without procedures in place for regularly reviewing enabled generic network user accounts, the District has a greater risk that unneeded access would not be detected and removed in a timely manner, and that access could be compromised or used for malicious purposes. In addition, unnecessary network user accounts are additional entry points into the District's network that attackers could potentially use to inappropriately access and view PPSI on the network.

Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such events.

Why Should District Officials Adopt an 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. An unexpected incident could include inadvertent employee action, a power outage, equipment destruction, a software failure caused by a virus or other type of malicious software or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such events.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the school district's computerized operations and IT environment. Proactively anticipating and planning for IT disruptions helps prepare 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.

Because key business processes often operate within computerized environments, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT contingency plan should focus on strategies for sustaining a school district's critical business processes in the event of a 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 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 district 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.

District Officials Did Not Develop an Adequate IT Contingency Plan

The District did not have an adequate IT contingency plan to describe how officials would respond to potential disruptions and disasters affecting the District's IT environment. Although the District had backup and disaster recovery procedures, they did not address the range of threats to the District's IT system. Also, they do not focus on sustaining critical business functions during and after a disruption. The procedures do not give specific details of restoration such as what resources are needed to recover in the event of an emergency. In addition, although the procedures document the roles and responsibilities of key personnel, the individuals in those positions were not provided training on what to do in the case of a potential disruption or disaster. Furthermore, the procedures were not tested to ensure key officials and District contractors understood their roles and responsibilities in a potential disruption or disaster situation.

Although the District had backup and disaster recovery procedures, they did not address the range of threats to the District's IT system.

Therefore, in the event of a disruption or a disaster, such as a ransomware attack (a type of malicious software designed to block access to a computer system until a sum of money is paid), employees and relevant contractors have insufficient guidance to follow to help resume, restore or repair and/or rebuild essential operations in a timely manner. Without an IT contingency plan, there is an increased risk that the District could lose important data and/or suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Both the IT Director and Assistant Superintendent for Business said that they were aware that the District does not have an adequate IT contingency plan. Initially, District officials were working on formalizing a disaster recovery plan.

However this was delayed due to the COVID-19 pandemic. Consequently, they stated their focus has changed to address the broader IT contingency plan. They stated the IT contingency plan is a high priority and is a part of their upcoming three-year Technology Plan. However, District officials should have had an IT contingency plan in place prior to the pandemic.

Without a comprehensive contingency plan in place that all responsible parties have been trained on and that is periodically tested for effectiveness, 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 operations if a system malfunction or other disruption occurs. IT disruptions can occur unexpectedly. As a result, important financial and other data could be lost, or the District could suffer a disruption to operations that depend on its computerized environment.

What Do We Recommend?

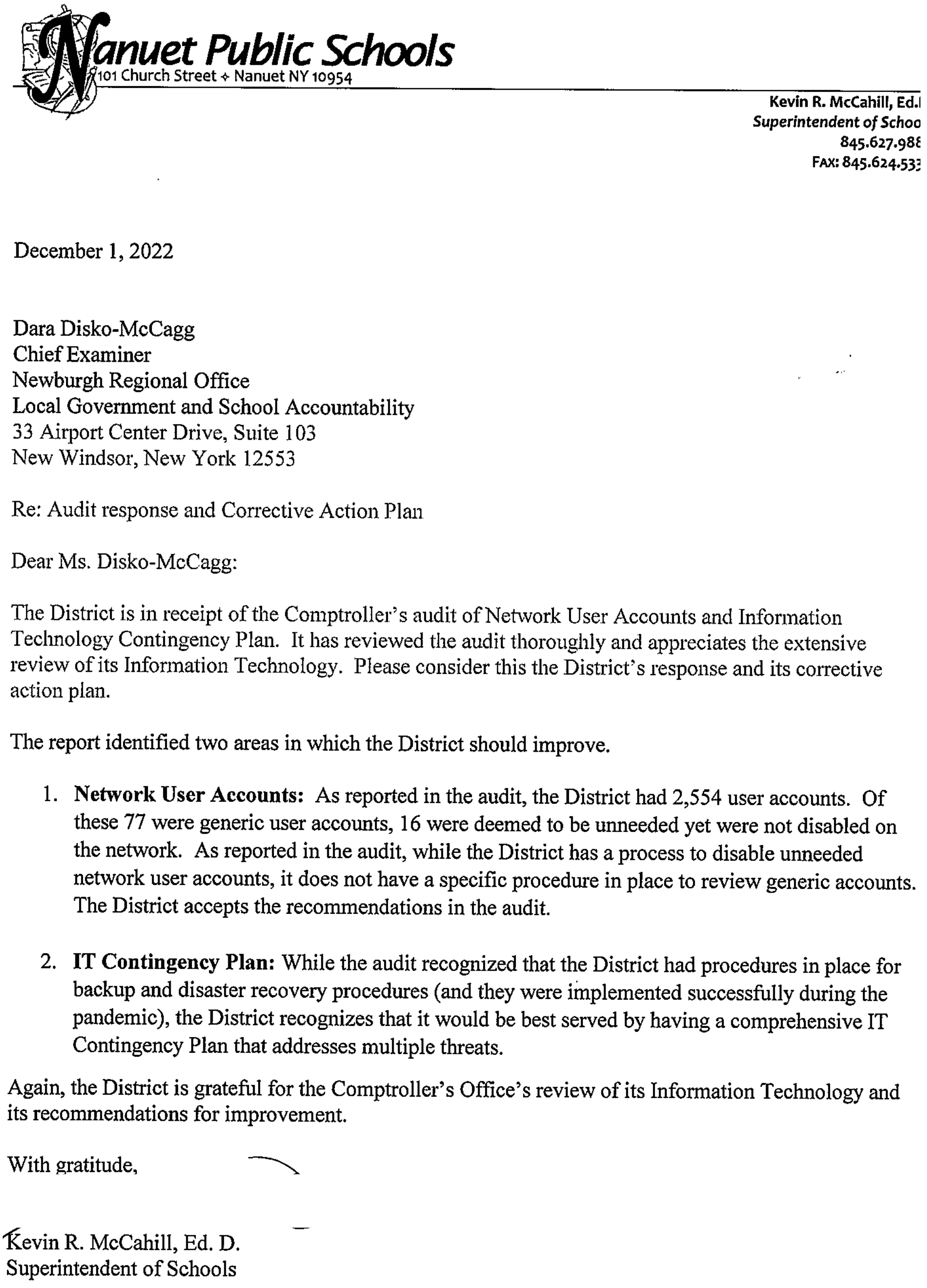
The Board should:

1. Develop, adopt and test an IT contingency plan that includes detailed guidance for continuing operations, key personnel and procedures for recovery of IT operations.

District officials should:

2. Develop adequate written procedures for managing generic network user accounts that include disabling generic user accounts as soon as they are no longer needed and periodically reviewing them for necessity and appropriateness.

Appendix A: Response From District Officials



Nanuet Public Schools
101 Church Street ✧ Nanuet NY 10954

Kevin R. McCahill, Ed.I
Superintendent of Schoo
845.627.98
FAX: 845.624.53

December 1, 2022

Dara Disko-McCagg
Chief Examiner
Newburgh Regional Office
Local Government and School Accountability
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Re: Audit response and Corrective Action Plan

Dear Ms. Disko-McCagg:

The District is in receipt of the Comptroller's audit of Network User Accounts and Information Technology Contingency Plan. It has reviewed the audit thoroughly and appreciates the extensive review of its Information Technology. Please consider this the District's response and its corrective action plan.

The report identified two areas in which the District should improve.

1. **Network User Accounts:** As reported in the audit, the District had 2,554 user accounts. Of these 77 were generic user accounts, 16 were deemed to be unneeded yet were not disabled on the network. As reported in the audit, while the District has a process to disable unneeded network user accounts, it does not have a specific procedure in place to review generic accounts. The District accepts the recommendations in the audit.

2. **IT Contingency Plan:** While the audit recognized that the District had procedures in place for backup and disaster recovery procedures (and they were implemented successfully during the pandemic), the District recognizes that it would be best served by having a comprehensive IT Contingency Plan that addresses multiple threats.

Again, the District is grateful for the Comptroller's Office's review of its Information Technology and its recommendations for improvement.

With gratitude,

Kevin R. McCahill, Ed. D.
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, employees and the LHRIC staff to gain an understanding of the District's IT operations. We also reviewed IT-related policies to gain an understanding of the network user accounts and determine whether the District had an adequate IT contingency plan.
- We used a computerized audit script to examine the District's domain controller on November 9, 2021.[2] We then analyzed the report to determine whether all enabled network user accounts were associated with individuals currently employed, contracted or enrolled in the District. We compared the list of network user accounts generated by the script to a list of current employees to determine whether any network users were no longer employed by the District. We discussed all accounts not verified as current employees with the IT Director.

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.

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

[2] The domain controller is the main server computer in the domain (network) that centrally manages all computers within the domain. It is responsible for allowing users to access network resources.

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 of Municipal Audits

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