New York State Comptroller
THOMAS P. DiNAPOLI

Syracuse City School District

Information Technology

2025M-129 | February 2026

Division of Local Government and School Accountability

Contents

Audit Results

Syracuse City School District

Audit Objective	Audit Period
Did Syracuse City School District (District) officials adequately manage nonstudent network user accounts and develop and adopt an information technology (IT) contingency plan?	July 1, 2024 – May 16, 2025

Understanding the Audit Area

School district officials must manage network user accounts and create IT contingency plans to help protect personal, private, sensitive student/staff information (PPSI),[1] prevent unauthorized access/breaches, ensure operational continuity during disasters, meet statutory requirements, and maintain public trust. Unmanaged network user accounts are potential entry points for attackers and other unauthorized individuals, and the lack of a contingency plan can paralyze a school district's operations. These measures help safeguard against financial loss and ensure critical functions continue, protecting the entire school district community.

As of November 15, 2024, the District had 6,386 enabled nonstudent network user accounts.

Audit Summary

District officials did not adequately manage nonstudent network user accounts. As of November 15, 2024, 488 of the District's 6,386 enabled nonstudent network user accounts (8 percent) were not needed and should have been disabled. We determined that 433 of the unneeded network user accounts (89 percent) had never been logged into or not been logged into for over six months. Furthermore, 157 service and shared user accounts had not been logged into for at least five years. In addition, 15 of 33 nonstudent network user accounts (45 percent) that had administrative permissions were unnecessary.

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 PPSI, make unauthorized changes to District records; or deny legitimate access to the District's network and

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 individuals or entities.

records. In addition, a compromised network user account with administrative permissions could cause greater damage than the compromised lesser privileged user account because administrative accounts have full control over the network, including the ability to add new users and change passwords and permissions.

IT department officials initiated corrective action during our audit to disable unnecessary nonstudent network user accounts. As of May 16, 2025, IT department officials disabled 371 of the 488 unneeded network user accounts (76 percent) identified during the audit.

In addition, the Board of Education (Board) and District officials did not develop and adopt an IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of services. As a result, officials have less assurance that, in the event of a disruption or disaster (e.g., a ransomware attack), employees and other responsible parties would be able to react quickly and effectively to help resume, restore, repair and/or rebuild critical IT systems or data in a timely manner.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes six recommendations that, if implemented, will improve the District's management of nonstudent network user accounts and contingency planning. District officials agreed with our recommendations and indicated they have initiated or plan to initiate corrective action, and their response is included in Appendix B.

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 (GML). Our methodology and standards are included in Appendix C.

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 GML, Section 2116-a (3)(c) of the 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.

Information Technology: Findings and Recommendations

To actively manage network user accounts, school district officials should periodically review user account access and permissions, including administrative permissions, to ensure access is appropriate and properly limited based on each user's current and assigned roles and responsibilities. When user accounts are no longer needed, they should be disabled immediately. Officials should develop written procedures to help guide network administrators in properly granting, changing and revoking user account access to the network. In addition, the board of education and school district officials should develop and adopt a written 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.

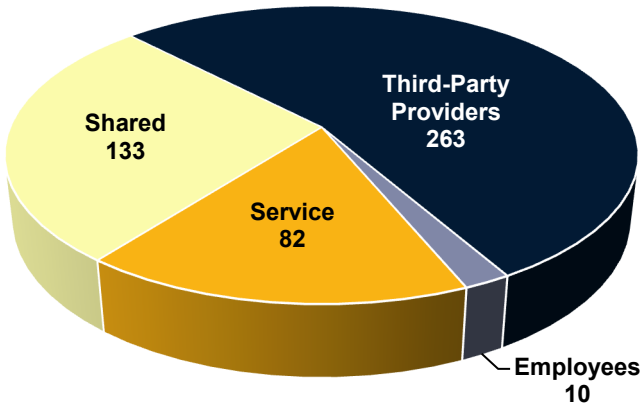
Nonstudent network user accounts include accounts assigned to school district employees, third-party service providers, and service and shared accounts.[2] When nonstudent network user accounts are not properly managed, there is an increased risk for unauthorized access to a network and unauthorized use of PPSI.

More details on the criteria used in this report, as well as resources we make available to help school district officials improve their operations, are included in Appendix A.

Finding 1 – District officials did not adequately manage nonstudent network user accounts to ensure all accounts were needed.

District officials did not adequately manage nonstudent network user accounts to ensure all accounts were needed. With the assistance of the Executive Director of Technology (Executive Director) and IT department officials, we reviewed all 6,386 enabled nonstudent network user accounts as of November 15, 2024. We identified 488 nonstudent network user accounts (8 percent) that were not needed and should have been disabled (Figure 1).[3] Of these unneeded nonstudent network user accounts, 433 accounts (89 percent) had either never been logged into or had not been logged into for over six months.

Figure 1: Unneeded Nonstudent Network User Accounts



2 Service accounts are accounts created for the sole purpose of running a particular network or system service or application. Shared accounts are accounts that are used by more than one user for the purpose of logging into a computer system and accessing network resources. For example, service accounts can be created and used for automatic backups, while shared accounts may be used for testing purposes, training purposes or for shared e-mail accounts, such as a service helpdesk account.

3 Fourteen of the 488 unneeded network user accounts had administrative permissions. See Finding 2 for additional details.

Third-Party Service Providers – We determined that 263 of the unneeded nonstudent network user accounts (54 percent) were assigned to third-party service providers. IT department officials created a third-party user account for each individual service provider that needed access to the District's network to perform or assist with District operations (e.g., vendors that provide educational and technical assistance). When a third-party service provider user account is created, IT department officials set an expiration date for the account which prevents the user from logging into the account after the expiration date. Although the user would not be able to log into the account after the expiration date, users with administrative permissions can still access the expired user accounts. This could be a risk because someone with administrative permissions could use this as an opportunity to access the network using a different user account other than their own. For example, a user with administrative access could use an expired user account with lesser privileges to cause disruptions to the network and conceal their malicious activity. There is also a risk that an attacker could successfully compromise an expired user account and use it to cause damage across the network. Therefore, even if network user accounts have expired, the accounts should still be disabled to reduce potential entry points into the District's network. Of the 263 unneeded nonstudent user accounts assigned to third-party service providers:

- 251 network user accounts were assigned to individuals who no longer provided services to the District, including 25 user accounts that were not used in at least five years and one user account that was not used in 16 years.
- 10 network user accounts were assigned to individuals who subsequently were hired by the District. When IT department officials created a new user account for these individuals for their new job title, their third-party service provider user account was not disabled.
- Two network user accounts were duplicate accounts assigned to two individuals.

The Executive Director told us that IT department officials reviewed third-party network user accounts in October 2024 and disabled all third-party user accounts that were not needed. However, during our audit fieldwork, he realized the review only included a subset of the third-party user accounts. Consequently, their review did not include all the unneeded third-party network user accounts we identified during our audit.

Service and Shared Accounts – We identified 215 service and shared user accounts that were no longer needed and should have been disabled, including 157 user accounts (73 percent) that had not been logged into for at least five years.

The shared network user accounts were created for various purposes, including temporary and guest accounts, and the service user accounts were for software programs used by District officials. The Executive Director told us the IT department did not have procedures to routinely review and monitor shared network user accounts, but they implemented procedures in April 2018 as part of a change management process to routinely review and monitor service network user accounts. However, these procedures were not adequate given that we identified 82 unneeded service network user accounts that were enabled.

Employees – We identified 10 network user accounts assigned to former District employees, including seven user accounts assigned to student teachers no longer with the District and three user accounts assigned to employees who separated from the District in May 2020. The Executive Director told us that IT department officials reviewed employee user accounts quarterly; however, he could not provide support showing the review was completed or how the review was performed. In addition, we determined that one user account was logged into after the date the account was last needed. This user account was accessed on June 15, 2020, 17 days after the date the account was last needed. The Executive Director could not explain why this user account was logged into after the date it was last needed, but indicated that no disruptions in services resulted from this access.

Although the District had written procedures for granting, changing and disabling user account access to the network for third-party service providers and employees, the District did not have written procedures for shared and service network user accounts. In addition, the District did not have written procedures for monitoring network user accounts to ensure all accounts are still needed. The Chief Information Officer (CIO) told us the IT department had higher-level priorities, such as implementing a new financial system and providing each student with their own device, which took priority over establishing written procedures for shared and service accounts and monitoring network user accounts.

Furthermore, IT department officials initiated a review of network user accounts in October 2023. However, this review was limited to user reports obtained from a third-party vendor that did not include all network user accounts and the Executive Director told us that the review was not completed. Therefore, many of the unneeded user accounts identified in our audit remained enabled.

Although officials took steps to review network user accounts at various times, the reviews were not always consistent and effective to identify accounts that were no longer needed. Developing written procedures for conducting periodic reviews of network user accounts could help to ensure that the IT department's reviews are thorough and complete to identify and remove unneeded user access.

During our audit fieldwork, the Executive Director told us that IT department officials started to disable the unneeded network user accounts identified in this report. We verified that as of May 16, 2025, 371 of the 488 unneeded nonstudent network user accounts (76 percent) were disabled. The Executive Director told us the IT department is working on disabling the remaining 117 unneeded user accounts.

When unneeded accounts remain enabled on a network, it could make network user account management more difficult and increase the chance for inadvertent errors to occur, such as not detecting user accounts that should be disabled or granting an account greater access than needed. Also, 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 network to view PPSI, make unauthorized changes to District records or deny legitimate access to the network and records.

Recommendations

The CIO should:

1. Develop written procedures for granting, changing and disabling shared and service network user accounts.
2. Establish written procedures and implement a system to periodically review all existing network user accounts to determine whether accounts are needed and properly disable unneeded accounts.
3. Disable all unneeded network user accounts identified in this report.

Finding 2 – Some nonstudent network user accounts with administrative permissions were unneeded or did not require administrative permissions.

We reviewed the necessity and appropriateness of all 33 nonstudent network user accounts that had administrative permissions and determined that 15 user accounts (45 percent) had unnecessary administrative permissions, including 14 user accounts[4] that were no longer needed and had unnecessary administrative permissions and one user account that was needed but did not need administrative permissions. A compromised network user account with administrative permissions could cause greater damage than a compromised lesser privileged user account because administrative accounts have full control over the network, including the ability to add new users and change passwords and permissions.

The IT department did not have written procedures to routinely review user accounts with administrative permissions and ensure the permissions were needed. IT department officials determined whether administrative permissions should be granted when the user accounts were created. The Executive Director told us that IT department officials performed a review of network user accounts with administrative permissions in October 2023, but did not complete the research necessary to determine the purpose of certain user accounts and whether the administrative permissions were needed. As a result, user accounts with administrative permissions remained enabled because the accounts needed further review.

Although IT department officials began a review of administrative permissions in October 2023, the review was inconsistent and incomplete to identify user accounts with unnecessary administrative permissions. Having written procedures to periodically review administrative permissions could help ensure user access is appropriate and identify when administrative permissions are no longer needed.

4 These 14 user accounts are included in the 488 unneeded nonstudent network user accounts identified in Finding 1.

During our audit fieldwork, IT department officials began taking steps to disable the unneeded network user accounts with administrative permissions that were identified. We verified that as of May 16, 2025, five of the 14 unneeded nonstudent network user accounts (36 percent) with administrative permissions were disabled.

When users have unneeded administrative permissions to the network, they could make unauthorized changes that might not be detected. In addition, attackers will often target and use accounts with administrative permissions 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.

Recommendations

The CIO should:

4. Establish written procedures to periodically review nonstudent network user accounts with administrative permissions to determine whether the accounts are needed and properly disable unneeded accounts.

5. Disable unneeded nonstudent network user accounts with administrative permissions and remove the unneeded administrative permissions for the user account identified in this report.

Finding 3 – 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. The Board adopted a policy directing the Superintendent of Schools (Superintendent), and/or a designee, to develop a disaster recovery plan, which is a component of an IT contingency plan. The CIO told us because of the higher level priorities stated in Finding 1, IT department officials did not create an IT contingency plan. Additionally, the Executive Director told us an IT contingency plan was not completed because the District's IT environment was expanding to include a new data center, and the plan would need to be updated to reflect the new changes. While an IT contingency plan would need to be updated to reflect any changes to the IT environment, the District should have a plan in place that can be used in the event of a disaster or other unexpected IT disruption.

Without an IT contingency plan, officials have less assurance that, in the event of a disruption or disaster (e.g., a ransomware attack), employees and other responsible parties would be able to react quickly and effectively to help resume, restore, repair and/or rebuild critical IT systems or data in a

timely manner. As a result, the District has an increased risk that it 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 maintain and update student grades.

Recommendation

6. The Board and District officials should develop and adopt a written IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Appendix A: Profile, Criteria and Resources

Profile

The District is located in the City of Syracuse in Onondaga County. The Board is composed of seven elected members who are responsible for the general management and control of the District's financial and educational affairs. The Superintendent is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District operates 36 schools with 17,642 students and 5,140 employees. The District's budgeted appropriations for the 2024-25 school year were $578 million, which are funded primarily with State aid and real property taxes.

As of November 15, 2024, the District had 28,422 enabled network user accounts, including 22,036 network user accounts assigned to students and 6,386 nonstudent network user accounts. The CIO is responsible for overseeing the IT department which provides centralized IT services throughout the District. The CIO, along with the Executive Director, is responsible for managing the District's IT network, including nonstudent user account access to the network. The IT department includes three network administrators who are responsible for adding, disabling and modifying user access rights, permissions and security settings.

Criteria – Information Technology

School district officials should adequately manage all network user accounts, including nonstudent network user accounts (e.g., employee, shared, service, and third-party vendor accounts), to minimize the risk of unauthorized network access. Adequate network account management means network access and permissions are only granted to individuals that need access, and their permissions are limited to what is needed to perform their job responsibilities. Officials should manage the creation, use and dormancy of network user accounts, and regularly monitor them to ensure they are appropriate and authorized. User accounts that are no longer needed should be disabled immediately. School district officials should have written procedures for granting, changing, disabling and monitoring user account access to the network. These procedures should establish who has the authority to grant or change user account access and require school district officials to periodically review enabled user accounts to ensure they are appropriate.

Nonstudent network user accounts with administrative permissions have oversight and control of the network, with the ability to add new users and change users' passwords and permissions. Users with network administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. Therefore, school district officials should limit users with administrative permissions and regularly monitor all user account access to ensure it is appropriate and authorized.

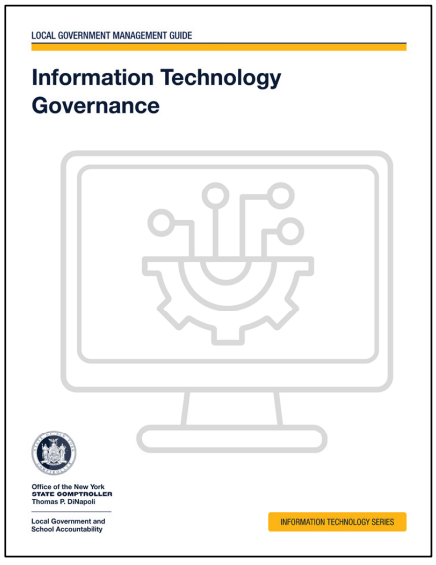
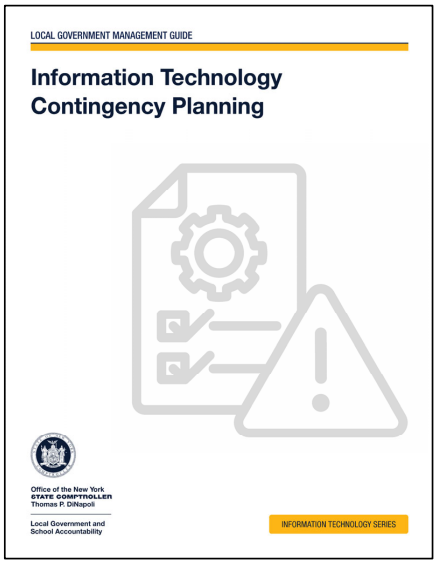
In addition, the board of education and school district officials should develop and adopt a written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. An IT contingency plan is a school district's 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 inadvertent employee action, power outage, ransomware or other types 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.

Typically, IT contingency planning involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to recover data and quickly resume operations in the event of an unplanned disruption. The plan should 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 in security requirements such as statutory changes.

Additional IT Resources

Figure 2: OSC Publications

OSC *Local Government Management Guides* available on our website to help officials understand and perform their responsibilities.

Information Technology Governance	*Information Technology Contingency Planning*
	
https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf	https://www.osc.ny.gov/files/local-government/publications/pdf/itcontingencyplanning.pdf

In addition, our website can be used to search for audits, resources, publications and training for officials: https://www.osc.ny.gov/local-government.

Appendix B: Response From District Officials

SYRACUSE CITY SCHOOL DISTRICT
Pamela J. Odom, Superintendent of Schools

Office of the Superintendent

February 10, 2026

Rebecca Wilcox, Chief of Municipal Audits
Office of the New York State Comptroller
Syracuse Regional Office
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Dear Ms. Wilcox:

The Syracuse City School District appreciates the opportunity to review and respond to the draft audit report "Information Technology – 2025M-129". We thank the audit team for their professionalism and collaboration throughout this process.

The District has reviewed and agrees with the recommendations of all three findings. The IT department began corrective actions during the audit, as noted in the report, and has continued these efforts. A separate Corrective Action Plan will be submitted within 90 days of the final audit report.

Thank you for the insights and recommendations provided. These findings will support our ongoing efforts to strengthen the District security practices and enhance our operational procedures.

Sincerely,

Pamela J. Odom
Superintendent of Schools

725 Harrison Street, Syracuse, NY 13210 | T (315) 435-4499 | syracusecityschools.com

Appendix C: Audit Methodology and Standards

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, CIO and Executive Director to gain an understanding of the District's IT environment, including procedures related to granting, changing, disabling and monitoring nonstudent network user accounts and permissions and to determine whether the District had an IT contingency plan.
- We ran a computerized audit script on the District's domain controller on November 15, 2024. We analyzed the script results to obtain information about the District's 6,386 enabled nonstudent network user accounts (including their permissions) to determine whether the accounts were necessary and appropriate. We compared the 6,386 enabled nonstudent network user accounts to employee master lists to identify unused and possibly unneeded network user accounts and to determine whether enabled network accounts were associated with District employees or third parties, or if they were shared or service accounts. Additionally, we followed up with District officials to assess whether the accounts with administrative permissions were needed. We ran a second computerized audit script on the District's domain controller on May 16, 2025 to determine whether unneeded network user accounts identified in our initial audit script were disabled.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

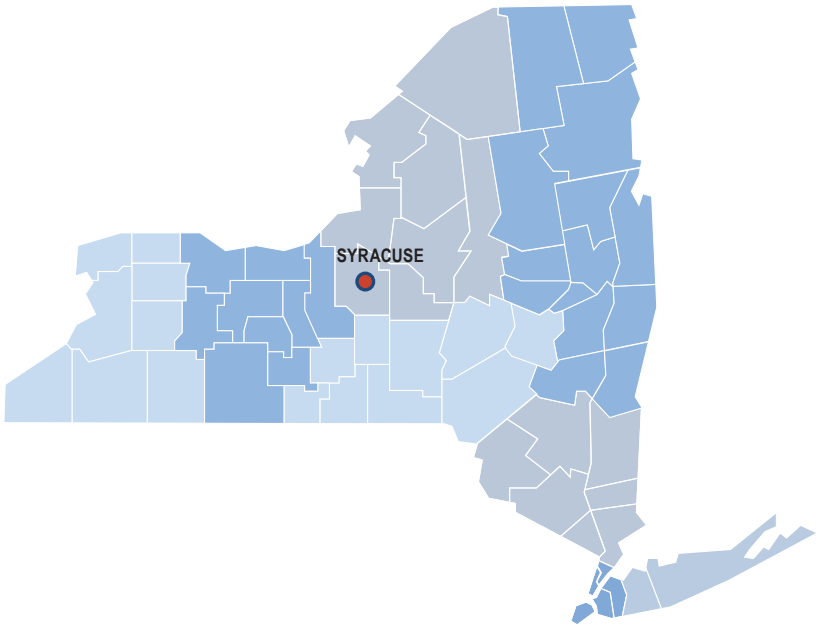
Contact

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



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