New York State Comptroller
THOMAS P. DiNAPOLI

Levittown Union Free School District

Information Technology

June 2026 | 2025M-145
Prepared by the Division of Local Government and School Accountability

Contents

Audit Results

Levittown Union Free School District

Audit Objective

Did Levittown Union Free School District (District) officials adequately manage nonstudent network accounts and permissions?

Audit Period

July 1, 2023 – March 6, 2025

Understanding the Audit Area

School districts rely on information technology (IT) systems (including IT assets and networks) for storing and processing important financial and non-financial information, accessing the Internet and communicating through email. These systems hold data that are valuable, such as (but not limited to) student and employee names, dates of birth, addresses, medical information and social security numbers. Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access and loss. Network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view personal, private, sensitive information (PPSI)[1] on the network, make unauthorized changes to official school district records or deny legitimate access to network resources.

The District's IT system includes 2,972 enabled nonstudent network user accounts.

Audit Summary

District officials did not adequately manage nonstudent network accounts and permissions. As a result, the District had an increased risk of unauthorized access, which could lead to loss of the District's data and network resources. The audit determined that officials did not:

- Disable five of 2,972 nonstudent user accounts that were no longer needed.
- Adopt a policy requiring the use of dedicated administrative accounts.
- Adopt a policy or procedures for software updates to help safeguard nonstudent network accounts and permissions.

By not adequately managing nonstudent network accounts and permissions, the District's network is at greater risk of cyberattacks and unauthorized access. In addition, by not having dedicated administrative accounts, there can be an increased risk of privileged accounts being exposed to attackers. Also, without a software update policy and procedures, officials have less assurance that outdated computer software will be identified and remediated in a timely manner. Outdated computer software potentially introduces nonstudent network accounts and permissions to the risk of being exploited by attackers who actively seek software known to have vulnerabilities and weaknesses.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

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.

The report includes five recommendations that, if implemented, will improve the District's management of nonstudent network accounts and permissions, and reduce the risk of unauthorized or inappropriate access. District officials generally agreed with our recommendations and plan to initiate corrective action.

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the Office of the New York State Comptroller's (OSC) 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

Nonstudent network accounts include user accounts and computer accounts, and both should be actively managed to minimize the risk of unauthorized use. To properly manage nonstudent network user accounts, there should be a policy and procedures for granting, changing and revoking access to the network. In addition, the policy and procedures should address nonstudent network user accounts with administrative privileges to ensure they are not used to conduct general computing activities, such as Internet browsing, that can be performed more securely by using separate lesser-privileged accounts.

Procedures should also have guidelines for properly patching computers, including installing standard updates within the industry recommended timeframe and applying critical or high security risk updates immediately or within accelerated timeframes defined by the policy. Patches are software updates released to address outdated computer software and resolve security vulnerabilities with software. Patches should be installed in a timely manner to ensure network computers remain secure from attackers who actively seek software known to have vulnerabilities and weaknesses.

More details on the criteria used in this report, as well as resources we make available to local officials that can help them improve operations, are included in Appendix A.

Finding 1 – District officials did not ensure all nonstudent network user accounts were necessary, and administrative user accounts were properly managed.

The District has a policy for creating and disabling nonstudent network user accounts that indicates nonstudent network user accounts are to be created when the Human Resources (HR) Department notifies the IT Director of a new employee. Access for a nonstudent network user account is granted based on the role and job duties of the individual. The policy does not address creating dedicated nonstudent network user accounts for users who need administrative privileges for certain job duties, or the management of independent contractors (contractors). To disable nonstudent network user account access for employees, the IT Department reviews Board meeting minutes and agendas for resignations, terminations and job role changes. The IT Department confirms the account user's last day of employment with the HR Department before disabling the nonstudent network user account. For contractors, the IT Director relies on a list provided once a year at the start of the school year, from the departments responsible for hiring the contractors, to create nonstudent network user accounts and disable the accounts no longer needed.

Nonstudent Network User Accounts – We identified and reviewed all 2,972 enabled nonstudent network user accounts to determine whether they were needed and had appropriate user permissions. We determined five nonstudent network user accounts were not needed and should have been disabled.

The IT Director said that the five nonstudent network user accounts were not disabled because he was not aware the users were no longer with the District. He said that four of the five nonstudent network user accounts were for contractors, and he was not aware of the contract-end dates for these individuals because of the District's procedure for notifying the IT Department. The District's method for determining when a contractor's nonstudent network user account should be disabled does not align with best practices. Nonstudent network user accounts should be disabled on the day the contractor leaves the District. The remaining nonstudent network user account was for an employee who left the District. The IT Director said that the IT Department was unaware that the account should have been disabled because notice of the employee's resignation was not included in Board meeting minutes or agendas as expected. Because the IT Department does not receive information directly from the HR Department and instead does their own review of Board meeting minutes and

agendas for resignations, terminations and job role changes, if a name is added after their review, nonstudent network user accounts for individuals no longer employed by the District could remain enabled.

Dedicated Administrative Accounts – Although all nonstudent network user accounts had appropriate permissions, the users with administrative permissions did not have dedicated administrative accounts and secondary, lesser-privileged accounts for tasks not requiring administrative access. Instead, these administrative accounts were used for both general computing activities as well as administrative duties. Because there is no policy that requires the use of dedicated administrative accounts, the IT Director did not create secondary, lesser-privileged accounts.

The IT Director told us that while he was aware that dedicated administrative accounts should be used, he could not explain why the IT Department had not created the secondary, lesser-privileged accounts for general computing activities.

Because the IT Department is unaware of contract-end dates and the HR Department does not notify the IT Department of an employee's last day of employment, IT staff may not disable nonstudent network user accounts on the day contractors and individuals leave the District, allowing nonstudent network user accounts to remain enabled.

When unused nonstudent network user accounts remain enabled, there is an increased risk of unauthorized access to the District's network. Former staff or other individuals could access sensitive systems, student records or internal communications. Furthermore, attackers could exploit unused nonstudent network user accounts to launch attacks within the District's network. Also, not having dedicated administrative accounts can increase the risk of privileged accounts being exposed to attackers. This exposure can lead to unauthorized access, allowing attackers to make changes to computer systems and the District's network.

Recommendations

The Board should:

1. Amend the policy for nonstudent network accounts to require the use of dedicated administrative accounts for users who need elevated privileges. The policy should also state that all general computing activities should be performed using lesser-privileged network user accounts.

The IT Director should:

2. Ensure written procedures are developed to require the HR Department to notify the IT Department before or on the same day an employee separates from service with the District.

3. Ensure written procedures are developed for departments that hire contractors who require network user accounts. The procedures should include notifying the IT Department of the contracted start and end dates, as well as prompt notification of the actual day the individual leaves the District to ensure that network user accounts are disabled in a timely manner.

Finding 2 – District officials did not have a policy or written patch management procedures to require computers be updated in a timely manner.

District officials have not adopted a policy or developed written procedures to require computer software updates be installed in a timely manner. Procedures for managing nonstudent network accounts should include steps to ensure servers and computers are patched in a timely manner, identify who is responsible for patching the servers and computers, and require monitoring servers and computers to ensure patches have been successfully applied. A patch can be an upgrade (adding features), computer bug fix, new hardware driver installation or an update to address new issues, such as security or stability problems. Although the IT Director

has a process to install patches to computers regularly, it is not memorialized in a written policy or written procedures. Once updates are pushed out, the Network Technician reviews the patch management system to verify that computers have successfully received the updates.

Because there is no patch management policy or documented procedures that define how often computers are patched, who is responsible for patching computers and how computers are monitored to ensure patches are applied successfully and regularly, there is an increased chance that computers could remain unpatched and the unpatched computers would not be detected in a timely manner.

When a computer is not updated regularly, there is a greater risk of cyberattacks and unauthorized access. Updates are crucial in addressing critical security risks, and without them, the system becomes an easy target for hackers and malicious software. Additionally, outdated systems can be exploited by attackers who actively seek known vulnerabilities. These events could have criminal, civil, regulatory, financial and reputational impacts on the District's operations. When officials do not establish a patch management policy or procedures, officials have less assurance that outdated computer software will be identified and remediated in a timely manner, potentially introducing the network to exploitation by attackers who actively seek software known to have vulnerabilities and weaknesses.

Recommendations

The Board should:

4. Establish a policy to require that patches be installed on devices within a defined number of days of released updates and aligns with industry best practices.

The IT Director should:

5. Develop and document procedures for how the IT Department will ensure updates are installed within a defined period of time, identify who is responsible for applying updates, and outline how computers should be regularly monitored to ensure updates are applied successfully.

Appendix A: Profile, Criteria and Resources

Profile

The District, governed by the elected seven-member Board of Education (Board), serves central Nassau County on Long Island, including parts of Levittown, Wantagh and Seaford. The District's fiscal year is from July 1 -June 30. The Board is responsible for the general oversight of the District's operations, which includes adopting policies to ensure security over the District's IT systems. The District has over 2,000 full-time and part-time employees, and 2,972 enabled nonstudent network user accounts.

The Board provides District employees and officials access to various computerized IT resources through the District's computer system consisting of software, hardware, computer networks and electronic communication systems. The District's IT system is used for Internet access, email and to maintain various records, such as financial, personnel and student records. The District uses network accounts, such as nonstudent user accounts and computer accounts, to control and manage access to the District's IT system and network resources.

The District's IT Department staff consists of the IT Director and six employees, one being the Network Technician, who is responsible for reviewing and ensuring computer updates are installed successfully. The IT Director is responsible for managing the IT Department, developing procedures and processes and overseeing the District's IT environment, including the management of network accounts and permissions and updates to servers, computers and software.

Criteria

A board of education should provide oversight and leadership by adopting IT policies that consider people, processes and technology. These policies should describe the tools and procedures used to manage nonstudent network accounts, help protect data and IT systems and assign key responsibilities.

Nonstudent network accounts are used to access the school district's network and include user accounts or computer accounts. Officials should actively manage the creation, use and dormancy of nonstudent network user accounts to minimize the risk of unauthorized use, access and loss. To properly manage nonstudent network user accounts there should be a policy in place for granting, changing and revoking access to the network. The policy should address procedures for regularly reviewing enabled nonstudent network user accounts to ensure they are still needed, disabling unneeded nonstudent network user accounts and removing unneeded user permissions. Nonstudent network user accounts should be disabled on the day network users leave school district employment. Disabling nonstudent network user accounts in a timely manner is important to prevent inappropriate access by unauthorized individuals.

When creating nonstudent network user accounts with administrative privileges, procedures should include steps to create dedicated administrative accounts as well as separate, lesser-privileged accounts for each user to conduct general computing activities such as Internet browsing, emailing, and productivity suite[2] use. Generally, a nonstudent network administrative account has elevated permissions to make system-wide changes, including creating new network accounts, installing programs and manipulating security settings. If an administrative network user account is compromised, an attacker would have administrative access to perform malicious activities.

Procedures for managing nonstudent network accounts should include steps to ensure servers and computers are patched in a timely manner, identify who is responsible for patching the servers and computers, and require monitoring servers and computers to ensure patches have been successfully applied. Patches update software programs and could help protect systems running those programs from attacks. A patch can be an

2 A collection of software applications used for producing information such as documents, presentations, worksheets, charts, and graphs.

upgrade (adding features), computer bug fix, new hardware driver installation or an update to address new issues, such as security or stability problems. Patches should be installed regularly – within current industry standards – to ensure network devices remain secure, or more immediately as required by patch severity. Updates are crucial in addressing critical security risks, and without them the IT system becomes an easier target for hackers and malicious software.

Additional Resources

OSC *Local Government Management Guides* and other informational resources that are available on our website to help officials understand and perform their responsibilities include:

- ***Information Technology Governance:*** https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf
- ***The Practice of Internal Controls:*** https://www.osc.ny.gov/files/local-government/publications/pdf/the-practice-of-internal-controls.pdf
- ***New York Local Government and School Cybersecurity:*** *A Cyber Profile*: https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-school-cyber-profile.pdf

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

Appendix B: Response From District Officials

The content below is a reproduced copy of the original response letter issued by District officials and is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[3] and may have included changes to spelling and grammar. The substance of the content was not changed.

LEVITTOWN PUBLIC SCHOOLS
Levittown Memorial Education Center
150 Abbey Lane
Levittown, NY 11756

April 21, 2026

Office of the NYS Comptroller
Hauppauge Regional Office

Ira McCracken
Chief of Municipal Audits
NYS Office Building, Room 3Al0
250 Veterans Memorial Highway
Hauppauge, NY 11788-5533

Mr. Todd Winch, Superintendent of Schools
Levittown Union Free School District
Report Title: Information Technology Audit - Report of Examination Report
Number: 2025M - 145

Dear Ira McCracken,

Levittown Union Free School District is in receipt of the *Information Technology Draft Audit Report number 2025M-145.*

The Board of Education as well as District Administration appreciate the diligent work and resulting recommendations provided by the Office of the State Comptroller (OSC). While we do feel our network accounts are adequately managed, we welcome the recommendations cited in the report as an opportunity to improve upon our policies and procedures. We are committed to keeping our District cybersecure and reducing risks whenever possible.

The District would like to thank the OSC staff assigned to this audit for their knowledge, input, and professionalism throughout the audit process.

Sincerely,

Todd Winch
Superintendent of Schools

3 https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule

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 IT Director to gain an understanding of nonstudent network account management.

- We ran computerized audit scripts on the District's network on November 6 and 7, 2024 to obtain account permissions and access on all nonstudent network user accounts. We identified 2,972 enabled nonstudent network user accounts and examined account permissions and settings using the reports generated by the computerized audit scripts.

- We obtained a list of all current District employees from the Payroll Department for use in our test to match enabled nonstudent network user accounts to active employees and compared the list to the nonstudent network user accounts.

- We followed up with the IT Director, payroll supervisor and accounts payable clerk to discuss inconsistencies between the active employee list and nonstudent network user accounts.

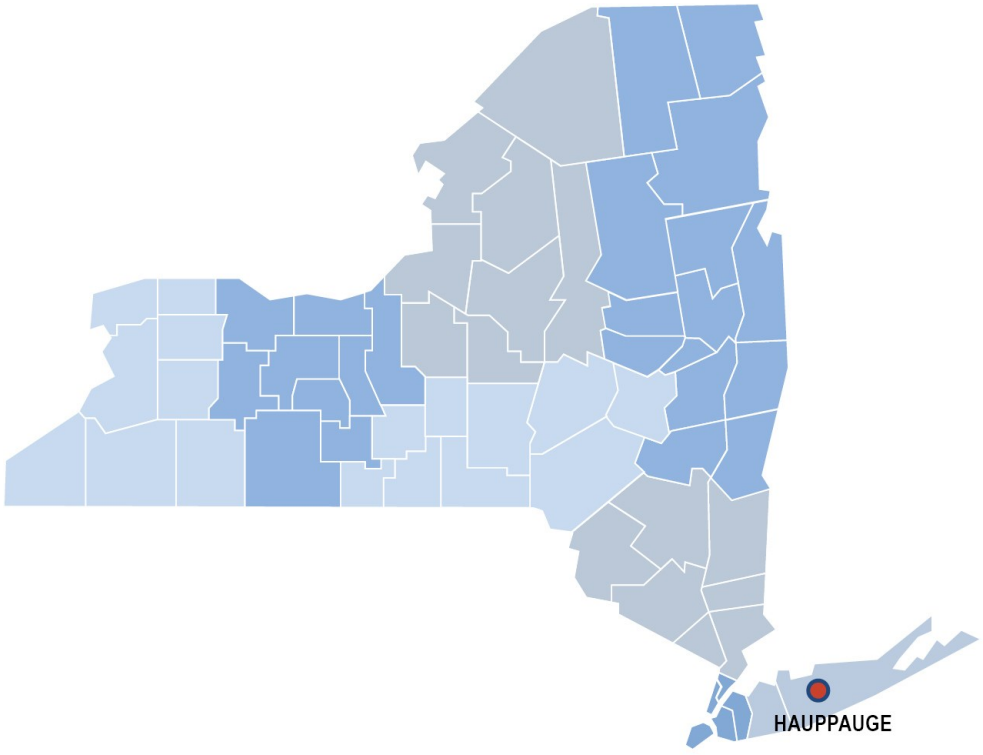
- We interviewed the IT Director and the Network Technician to obtain a more in-depth explanation of the District's patch management process.

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.

Questions?

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief of Municipal Audits
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534
Fax (631) 952-6091
Email: Muni-Hauppauge@osc.ny.gov
Serving: Nassau, Suffolk counties



Contact

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

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability