New York State Comptroller
THOMAS P. DiNAPOLI

Lawrence Union Free School District

Information Technology

September 2026 | 2026M-56

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Lawrence Union Free School District

Audit Objective

Did Lawrence Union Free School District (District) officials adequately manage network user accounts and provide IT security awareness training to staff?

Audit Period

July 1, 2024 – April 28, 2026

Understanding the Audit Area

School officials are responsible for effectively managing network user accounts and providing periodic IT security awareness training to staff. Together, these measures strengthen a district's IT control environment by helping prevent unauthorized access; protecting personal, private, sensitive information (PPSI)[1] and critical systems; reducing the risk of operational disruptions and supporting the continuity of a district's operations. Effective IT governance also helps safeguard public resources and promote accountability, transparency and public trust.

As of March 26, 2025, the District had 494 enabled nonstudent network user accounts on one domain, and as of April 24, 2025, it had 175 enabled nonstudent network user accounts on a second domain.

Audit Summary

Although District training records support that officials generally provided IT security awareness training to staff we reviewed, officials did not adequately manage all nonstudent network user accounts. As a result, officials cannot be assured that District IT systems are secured and protected against unauthorized use.

District officials did not have written policies or procedures for user account management. We identified 250 unneeded user accounts which District officials should have disabled or removed, including 162 accounts of former employees, third-party providers and consultants, and 88 service accounts. Additionally, officials could not provide documentation demonstrating IT security awareness training was completed for one employee of the 10 employee records we reviewed.

The report includes five recommendations that, if implemented, will improve the District's management of network user accounts, strengthen cybersecurity governance and internal controls and better protect District information systems from unauthorized access and misuse. District officials generally agreed with our recommendations and have initiated, or indicated they planned to initiate corrective action.

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the Office of the New York State Comptroller's (OSC's) authority as set forth in Article 3 of the New York State General Municipal Law (GML). The audit's methodology and standards are included in Appendix C.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to OSC 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 the CAP, please refer to the OSC brochure, *Responding to an OSC Audit*

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.

Report, which was provided 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 user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access and loss. To actively manage nonstudent network user accounts, school district officials should disable any network user accounts that are no longer needed in a timely manner.

Routine IT security awareness training helps ensure personnel understand their responsibilities and procedures for safeguarding school district data from potential abuse or loss. Such training should cover key security concepts including the dangers of downloading files and programs from the Internet or portable devices; the importance of selecting strong passwords; requirements related to protecting PPSI; wireless network connections; and how to respond if a computer virus or an information security breach is detected.

A formally developed IT contingency plan provides guidance for continuing and recovering IT operations after a major, unplanned incident such as loss of data due to unauthorized network access or a natural disaster.

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

Finding 1 – District officials did not adequately manage all nonstudent network user accounts.

The District did not have written procedures or a written Board-approved policy for user account management. We reviewed all 669 nonstudent network user accounts and identified 250 unneeded user accounts which District officials should have disabled, including 162 accounts of former employees, third-party providers and consultant accounts, and 88 service accounts.[2] Although the Information Systems and Technology Department Team-Lead told us that he monitored network user accounts for unusual activity, no process was in place to periodically review the necessity of these accounts. As a result, unnecessary network accounts remained enabled, which increased the District's risk of creating additional entry points into the network that could allow unauthorized access to PPSI and potential compromise of IT resources.

The Chief Information Officer (CIO) and Team-Lead told us that the District had not established procedures for the Human Resources Department to notify the Information Systems and Technology Department when employees and contractors left the District. After we communicated these findings to District officials, they implemented a new procedure, developed in collaboration with the Human Resources Department, that uses a tracking form for incoming and outgoing staff and contractors to ensure timely assignment and removal of network access.

Recommendations

The CIO should:

1. Develop a formal user account management policy that defines how accounts are created, modified, reviewed and disabled.
2. Enforce timely deactivation of accounts.

2 Service accounts are not linked to individual users and may be needed for certain network services or applications to run properly. Therefore, they should be limited in use as they have reduced accountability. For example, service accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk. Officials should routinely evaluate and disable any service accounts that are not related to a specific district or system need.

3. Perform periodic user access reviews to identify and disable inactive or unnecessary accounts.

The Board should:

4. Adopt a formal user account management policy.

Finding 2 – The Board generally provided IT security awareness training to employees

We reviewed the District's IT security awareness training materials to determine whether the training content was sufficient and completed by employees.

We determined that the training materials adequately addressed emerging trends that could compromise PPSI and data. We selected 10 employees to verify training completion. The District's Human Resources Department provided documentation demonstrating training completion for nine employees but was unable to provide documentation for one employee.

Verifying completion of IT security awareness training is important because trained employees are better equipped to recognize and respond to cybersecurity threats such as phishing, malware and unauthorized access attempts. Missing or incomplete training records reduce the District's assurance that all staff are adequately prepared to protect sensitive data and systems.

Recommendation

5. The CIO should collaborate with the District's Human Resources Department to ensure IT security awareness training completion is consistently documented and retained for all employees.

Appendix A: Profile, Criteria and Resources

Profile

The District is located in the Town of Hempstead in Nassau County. The Board is composed of seven elected members and is 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 Assistant Superintendent for Business and Operations (Assistant Superintendent) is responsible for overseeing and managing financial operations and serves as the appointed records management officer.

The CIO is responsible for overseeing the Information Systems and Technology Department, which provides centralized IT services throughout the District, including managing the District's IT network and nonstudent user account access to the network. The Team-Lead is responsible for adding, disabling and modifying user access rights, permissions and security settings. The District contracts with an outside vendor for onsite IT support.

Criteria

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 is only granted to individuals that need access. Officials should manage the creation, use and dormancy of network user accounts and regularly monitor them to ensure they are appropriate and authorized. Unneeded user accounts should be immediately disabled. School district officials should have written procedures for granting, disabling and monitoring user account access to the network.

Routine IT security awareness training helps ensure personnel understand their responsibilities and procedures for safeguarding district data from potential abuse or loss. Training should include key security concepts that include email security; the importance of selecting strong passwords; mobile device security; requirements related to protecting PPSI; risks involved with using unsecured wireless network connections; and how to respond if a computer virus is detected.

Additional Resources

OSC's *Local Government Management Guides,* and other informational resources that are available on OSC's 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

In addition, local officials can use OSC's 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, 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.

Lawrence Union-Free School District
2 Reilly Road
Cedarhurst, NY 11516
www.lawrence.org

September 9, 2026

Lawrence Union Fre School District
Response to Office of the New York State Comptroller Information Technology Audit
Report #2026M-056

The Lawrence Union Free School District appreciates the opportunity to respond to the findings and recommendations contained in the Office of the New York State Comptroller's Information Technology audit.

The District takes the security of its information systems, data, and technology resources seriously and is committed to maintaining strong internal controls and cybersecurity practices. We appreciate the Comptroller's review and the recommendations provided to further strengthen the District's management of network user accounts and documentation of information technology security awareness training.

The District is pleased that the audit recognized that its IT security awareness training materials adequately addressed emerging cybersecurity risks and that documentation was available demonstrating completion of the required training for nine of the ten employees selected for review. The District also acknowledges the opportunities identified by the auditors to strengthen user account governance and related documentation.

The District's responses to the five recommendations are as follows:

Recommendation 1
The CIO should develop a formal user account management policy that defines how accounts are created, modified, reviewed and disabled.

District Response:
The Chief Information Officer will develop a comprehensive user account management policy and supporting procedures governing the creation, modification, periodic review, and deactivation of network user accounts. The policy will address employee, contractor, third-party, shared, and service accounts and will establish clear roles and responsibilities for the departments involved in account management. Once finalized, the proposed policy will be presented to the Board of Education for review and adoption.

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

Recommendation 2
The CIO should enforce timely deactivation of accounts.

District Response:
The District began corrective action during the audit process. In collaboration with the Human Resources Department, the Information Systems and Technology Department implemented a tracking procedure for incoming and departing employees and contractors to facilitate the timely assignment and removal of network access.

The District will continue to formalize and monitor this process to ensure that notification of separations and changes in employment or contractual status is communicated promptly to Information Technology personnel and that network access is disabled when it is no longer required.

Recommendation 3
The CIO should perform periodic user access reviews to identify and disable inactive or unnecessary accounts.

District Response:
The Information Systems and Technology Department will establish a documented process for periodically reviewing enabled nonstudent network accounts to verify that each account continues to serve an authorized District or system need. These reviews will include employee, contractor, third-party, shared, and service accounts. Accounts determined to be inactive, obsolete, or otherwise unnecessary will be disabled or removed as appropriate. The District will also maintain documentation of these reviews to demonstrate ongoing compliance with its user account management procedures.

Recommendation 4
The Board should adopt a formal user account management policy.

District Response:
Following development and administrative review of the user account management policy described in Recommendation 1, the policy will be submitted to the Board of Education for consideration and formal adoption. The policy will establish the governance framework for managing network access throughout the District and will identify expectations regarding account authorization, creation, modification, review, and timely deactivation.

Recommendation 5
The CIO should collaborate with the District's Human Resources Department to ensure IT security awareness training completion is consistently documented and retained for all employees.

District Response:
The Chief Information Officer and Human Resources Department will strengthen their existing coordination to ensure that completion of required IT security awareness training is consistently tracked, documented, and retained for all applicable employees.

The District will establish a standardized documentation and record-retention process so that training completion can be readily verified. The District will also periodically reconcile training records to identify employees with missing or incomplete documentation and take appropriate follow-up action.

Conclusion
The District appreciates the Comptroller's recommendations and views the audit as an opportunity to further strengthen its cybersecurity governance and internal controls. Corrective actions have already begun in certain areas, and the District will continue working to implement the recommendations outlined above.

The District will incorporate these actions into its Corrective Action Plan and will continue to evaluate its information technology practices to safeguard District systems, sensitive information, and public resources.

The five formal recommendations are stated on pages 3-4 of the report. The report also requires a written Corrective Action Plan within 90 days, with implementation beginning by the end of the next fiscal year to the extent practicable.

Jeremy Feder
Assistant Superintendent of Business & Operations

Appendix C: Audit Methodology and Standards

OSC auditors obtained an understanding of internal controls that were deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of the work on internal controls, as well as the work performed in the 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, Assistant Superintendent, CIO and Team-Lead to gain an understanding of the District's IT environment, including procedures related to granting, disabling and monitoring nonstudent network user accounts.
- We ran a computerized audit script on the District's domain controllers on March 26, 2025 and April 24, 2025. We analyzed the script results to obtain information about the District's 669 enabled nonstudent network user accounts to determine whether the accounts were necessary and appropriate. We compared the 669 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 whether they were shared or service accounts.
- We used our professional judgment to select 10 out of 320 District employees and reviewed supporting documentation to determine whether they completed IT security awareness training. Our selection was based on a variety of titles and employees expected to have access to PPSI.

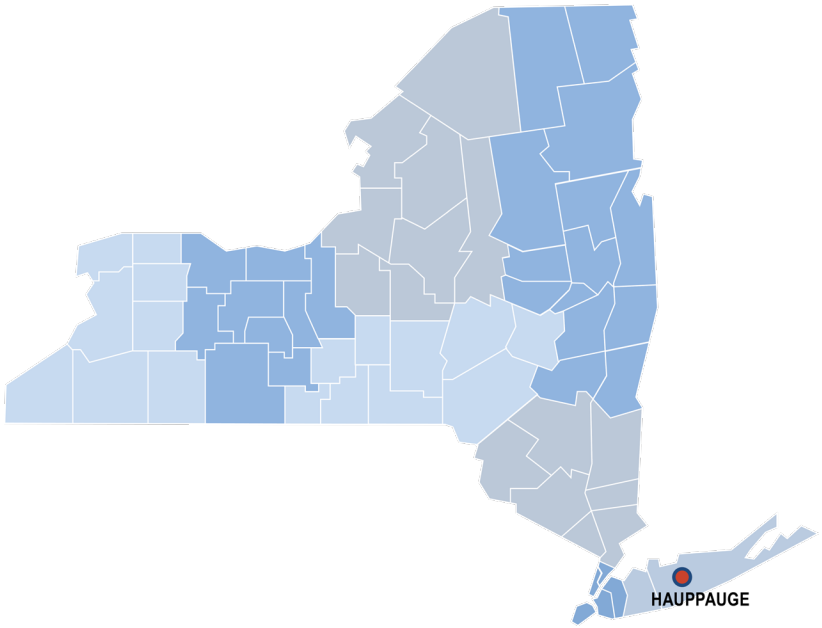
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the 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 relevant population size and the sample selected for examination.

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

https://www.osc.ny.gov/

Prepared by the Division of Local Government and School Accountability

NYS FOLLOW US: osc.ny.gov/subscribe