New York State Comptroller
THOMAS P. DiNAPOLI

Copiague Union Free School District

Information Technology

2023M-150 | March 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Copiague Union Free School District

Audit Objective

Determine whether Copiague Union Free School District (District) officials properly managed nonstudent network user accounts and financial software access controls.

Key Findings

District officials did not properly manage nonstudent network user accounts and financial software access controls. As a result, data and personal, private and sensitive information (PPSI) accessible by those accounts were at a greater risk for unauthorized access, misuse or loss. In addition to sensitive information technology (IT) control weaknesses that were confidentially communicated to District officials, we found that officials did not:

- Disable 316 nonstudent network user accounts (24 percent) that were not needed, including two user accounts assigned to employees that left the District more than 17 years ago.
- Ensure that employees had the appropriate access to the financial software necessary to perform their job functions.
- Provide IT security awareness and data privacy training annually to all officials and employees with access to financial and other sensitive data.

Key Recommendations

- Disable network and financial software user accounts as soon as they are no longer needed and periodically review accounts and access for necessity.
- Provide periodic data privacy and IT security and awareness training to officials and employees with access to PPSI.

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

Audit Period

July 01, 2021 – October 31, 2022

Background

The District serves the Town of Babylon in Suffolk County and is governed by an elected seven-member Board of Education (Board) responsible for managing and controlling financial and educational affairs.

The Superintendent of Schools is the chief executive officer and is responsible, along with the Assistant Superintendent for Finance and Operations (Assistant Superintendent) and other administrative staff, for the District's day-to-day management under the Board's direction. The Assistant Superintendent, as system administrator, is responsible for managing user access rights in the financial software.

The IT Director is responsible for managing the District's computer resources and overseeing the IT department, including the Network Engineer and technicians who manage the network and IT assets. The former IT Director resigned in August 2022, and the current IT Director started after the end of the audit period.

Quick Facts

Enabled Nonstudent Network User Accounts	
Individual	1,074
Service	99
Shared	126
Total	**1,299**

Information Technology

How Should Officials Manage Nonstudent Network and Financial Software Access Controls?

To help minimize the risk of unauthorized network access, misuse or loss, school district (district) officials should actively manage network user accounts and periodically conduct a user account review. Any account that cannot be associated with a current authorized user or district need should be disabled. District officials should have written procedures in place to grant, change and disable user account access to the network. These procedures should establish who has the authority to grant or change user access. Unneeded network user accounts should be disabled immediately when access is no longer needed.

Shared and service network user accounts should be limited in use as they are not linked to one individual and school district officials may have difficulty linking any suspicious activity to a specific user. A shared user account has a username and password that is shared among two or more users and is used to, for example, provide access to guests or other temporary or intermittent users. A service account is created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems). District officials should routinely evaluate the need for the accounts and disable those that are not related to a current district or system need.

When financial software is used to process transactions and maintain financial records, controls over access rights should allow users to access only those functions and data that are consistent with their job duties and responsibilities. Access rights should be periodically reviewed to help ensure adequate segregation of incompatible duties to prevent users from being involved in multiple phases of financial transactions. When possible, the financial software administrator should not be involved in financial operations because an individual who has administrative rights to the software can generally add new users, configure software settings, override management controls, change user access rights, and record and adjust financial transactions.

Officials Did Not Properly Manage Nonstudent Network and Financial Software Access Controls

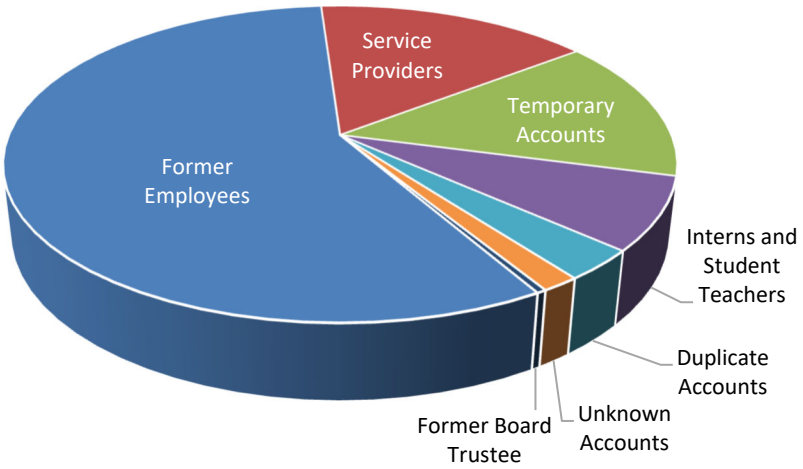
IT department and business office officials did not actively manage network or financial software user account access. District officials did not develop written procedures for granting, changing or disabling nonstudent network user accounts or to periodically review the necessity of nonstudent user account access to the network or financial software. Because there were no written procedures, the process for disabling nonstudent network user accounts was not consistent, especially for accounts assigned to individuals not employed by the District. As a result, the District had unnecessary nonstudent network user accounts and individuals with unneeded user access rights in the financial software.

We reviewed all 1,299 enabled nonstudent network user accounts, including 1,074 individual nonstudent accounts and 225 service and shared accounts. We determined that 316 network user accounts (24 percent) were not needed and should have been disabled.

Individual Nonstudent Network User Accounts – We compared the enabled nonstudent network user accounts to payroll data, and after discussing the accounts with District officials, we determined that 255 individual nonstudent user accounts (Figure 1) were unnecessary and should have been disabled, including:

FIGURE 1

Unneeded Nonstudent Network User Accounts



- 146 accounts assigned to former District employees, including accounts assigned to two employees who have not worked for the District for over 17 years.
- 40 accounts assigned to service providers who no longer worked for the District, including three accounts with administrative rights that could have been used to create new network user accounts and manipulate the security settings configured on the network. If one of these network administrative accounts was compromised, an attacker would have the same administrative permissions as the compromised account.
- 37 temporary accounts that were created on June 29, 2021 for a teaching assistant training program and never accessed. The Network Engineer said the users assigned to these accounts were not on the premises and did not log into the network.

- 19 accounts for former interns and student teachers who no longer needed access.
- Eight duplicate user accounts, including two enabled accounts assigned to a former employee that has not worked for the District in over six years.
- Four user accounts that District officials could not explain the purpose for their creation. District officials disabled these accounts after we brought them to their attention. Two of these accounts were never accessed, and the other two accounts were last accessed in 2016.
- One account assigned to a former Board trustee who has not served on the Board since 2021.

Although these accounts were disabled after we brought it to their attention, District officials should have disabled the accounts as soon as they were no longer needed, such as when the individuals left District employment or stopped providing services to the District. Because the District did not have procedures to routinely review and disable network user accounts, these accounts were not disabled and could potentially have been used by those individuals or others for malicious purposes.

Shared and Service Network User Accounts – We analyzed the last logon dates of all enabled shared and service network user accounts and requested that the Network Engineer review the 163 accounts we identified that were not used to access the network in over six months, including 25 accounts that have never been used and one account not used to access the network in 14 years. The Network Engineer said that 56 of these accounts were unnecessary and created for various purposes, such as testing and temporary accounts. The Network Engineer disabled the 56 accounts, and also deleted five additional shared network user accounts that had been used within the last six months but were no longer necessary.

Unnecessary nonstudent network user accounts, including service and shared accounts, were enabled on the network because District officials did not have adequate procedures to disable accounts when they were no longer needed and or periodically review accounts for access and necessity. The Network Engineer, Assistant Superintendent and current IT Director reviewed the enabled nonstudent network accounts at our request and told us they disabled the accounts we brought to their attention that they deemed unnecessary. Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could be used to inappropriately access and view PPSI accessible to that account.[1] Additionally, when District officials have to manage and review

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could be used to inappropriately access and view PPSI...

1 PPSI is any information to which unauthorized access, disclosure, modification, or use – or disruption of access or use – could have or cause a severe impact on critical functions, students, employees, customers or third-party entities.

many network user accounts, unneeded user accounts may make it difficult to manage network access.

Unnecessary Financial Software Access Rights – We reviewed the financial software user access rights for 11 financial software user accounts assigned to 10 employees to determine whether District officials appropriately controlled access in the software. We determined that the Assistant Superintendent and four business office employees had unnecessary access rights that allowed them more access than needed to perform their job duties and responsibilities. The unneeded access rights in the financial software included:

- The Assistant Superintendent had two financial software user accounts, one for day-to-day duties and one as system administrator. However, the account used for day-to-day duties had unnecessary access to modify information in the accounting, human resources and payroll modules. Because the Assistant Superintendent's duties included oversight of these areas, access to modify transactions should be limited. When an individual has the ability to perform multiple phases of a transaction within the financial software, it increases the risk that inappropriate transactions could occur and remain undetected.
- The Treasurer had unnecessary access to modify information in the human resources and payroll modules. In addition, the Treasurer had the ability to record collections, which was incompatible with her duty of preparing bank reconciliations.
- The Deputy Treasurer had unnecessary access to modify information in the human resources and payroll modules. In addition, the Deputy Treasurer had the ability to record collections, which was incompatible with his duties involving the reconciliation of accounts.
- A payroll clerk had unnecessary access to modify information in the human resources module.
- A benefits clerk had unnecessary access to create, delete and update information in the payroll module.

Although the Assistant Superintendent was the only system administrator of the financial software, she was not independent of financial operations. The Assistant Superintendent said that as system administrator, she would generally be contacted by administrators or the Human Resources department when an employee needed access to or removal from the financial software. However, having another District official, who is independent of the District's financial operations, serve as system administrator and be notified when there are staffing changes that require changes to an employee's access rights in the financial software would provide a better segregation of incompatible duties. The Assistant Superintendent said that her use of both the system administrator and day-to-

day user accounts was meant to serve as a mitigating control in the financial software. The Assistant Superintendent also provided us with documentation that the District's internal auditor performed a periodic review of her user activity trails for both user accounts as a mitigating control. However, it is not clear how often or in-depth these reviews were performed. While two user accounts and a review performed by the internal auditor may have helped to mitigate some risk of inappropriate transactions, there was still a risk because the Assistant Superintendent's system administrator accounts had unlimited access in the financial software and the day-to-day account had the ability to control all phases of a transaction.

The Assistant Superintendent stated that her predecessors set up the user access rights for the financial software accounts, and since taking the position in 2021, she has attempted to reduce user access to be compatible with an employee's job responsibilities. However, we determined that business office staff user access rights were not consistent with their assigned job duties and responsibilities. By not properly restricting user account access rights within the financial software, there are increased opportunities for users to access and make unauthorized and improper changes or modify accounting records to conceal malicious transactions. Furthermore, unnecessary access to payroll and human resources data could allow individuals to inappropriately view and misuse confidential information.

Studies show that human error accounts for a significant share of all cybersecurity breaches.

Why Should Officials Provide Data Privacy and IT Security Awareness Training?

Studies show that human error accounts for a significant share of all cybersecurity breaches.[2] Therefore, to help safeguard computerized data and help minimize the risk of unauthorized access and misuse or loss of data and PPSI accessible through nonstudent network user accounts and financial software access, district officials should ensure periodic data privacy and IT security awareness training is provided that explains rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all officials and employees. The training could center on, but not be limited to, emerging trends such as information theft and social engineering attacks (methods used to deceive users into revealing confidential or sensitive information), computer viruses and other types of malicious software, all of which may result in PPSI compromise.

The training should cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related

2 https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Awareness%20Month%202021%20-%20Approaching%20Cybersecurity%20Tip%20Sheet.pdf

to protecting PPSI; risks involved with using unsecured Wi-Fi connections; and how to respond if a computer virus or an information security breach is detected.

District Officials Did Not Provide Data Privacy and IT Security Awareness Training to All Staff

The District adopted a policy for information security breaches and data security that required officials to provide annual training on data privacy and IT security awareness to all officials and employees who have access to student and teacher/principal PPSI. We determined that IT security awareness training was provided to administrators and educational staff, including the Assistant Superintendent. However, business office staff were not provided IT security awareness training to ensure they understand IT security measures and their roles in safeguarding data, which they may access through their nonstudent network user accounts or financial software, from potential abuse or loss and protecting the District's network and IT assets. As a result of our audit inquiry, District officials provided IT security awareness training to the business office staff. Additionally, District officials did not provide data privacy training to officials and employees, resulting in staff not being informed of the requirements related to protecting PPSI.

Without providing periodic comprehensive data privacy and IT security awareness training, network users may unintentionally expose the District's network to unauthorized access and threats from malicious software that places District data, including PPSI, at risk.

What Do We Recommend?

The IT Director and District officials should:

1. Establish comprehensive written procedures for managing network user accounts, including how to grant, change and disable user access.
2. Ensure that nonstudent network user accounts are disabled as soon as they are no longer needed and periodically review and update the accounts for access and necessity.
3. Consider establishing a financial software system administrator who is not involved in the District's financial operations and review financial software user access rights for necessity and appropriateness.
4. Ensure that all officials and employees with access to PPSI receive annual data privacy and IT security awareness training in accordance with District policy.

Appendix A: Response From District Officials

COPIAGUE
PUBLIC SCHOOLS

Dr. Kathleen Bannon, Superintendent of Schools

Copiague Union Free School District

Information Technology

Report of Examination

2023M-150

February 28,2024

While there were no breaches during the time frame covered in this audit, we appreciate the information provided by the Comptroller's Office. The areas addressed on our corrective action plan will assist us in strengthening and improving our network.

RESPONSE AND CORRECTIVE ACTION PLAN:

Audit Period

July 01, 2021 – October 31, 2022

Recommendations from the Audit

The IT Director and District officials should:

1. Establish comprehensive written procedures for managing network user accounts, including how to grant, change, and disable user access.

   RESPONSE AND CORRECTIVE ACTION PLAN:

   Copiague UFSD is in the process of documenting and finalizing a user access management process that includes procedures for granting, modifying, and terminating user access.

2650 Great Neck Road • Copiague, New York 11726 • 631-842-4015 • Fax 631-841-4614

As part of the new process, all user access requests must be initiated and tracked via a helpdesk ticket and go through the assigned review, approval, and authorization process.

Copiague UFSD will implement procedures to review privileged and admin accounts and access at least quarterly, and regular user accounts/access at least annually.

In addition, Copiague UFSD will perform access reviews of systems and applications deemed critical, via the Business Impact Analysis, at least quarterly.

These access management procedures shall be finalized and implemented no later than July 1, 2024.

2. Ensure that nonstudent network user accounts are disabled as soon as they are no longer needed and periodically review and update the accounts for access and necessity.

RESPONSE AND CORRECTIVE ACTION PLAN:

As part of the updated access management process to be formalized, HR will immediately initiate all terminations in a help desk ticket which will travel through the appropriate transaction flow, includes email notifications to those responsible, to disable users from their accounts and access to systems, applications, and the physical locations within the district.

All terminated employees accounts and access, whether voluntary or for cause, shall be disabled no later than 24 hours after initiation of the ticket and audited by the IT Director within 24 hours to ensure all access has been disabled.

These access management procedures shall be finalized and implemented no later than December 31, 2024.

3. Consider establishing a financial software system administrator who is not involved in the District's financial operations and reviews financial software user access rights for necessity and appropriateness.

RESPONSE AND CORRECTIVE ACTION PLAN:

The responsibility for the financial application will be under the purview of a Central Office Administrator other than the Assistant Superintendent for Finance and Operations.

The district shall also incorporate the following compensating controls to reduce the risk of inappropriate access:

- As part of the new access management process, all additions, changes, and/or terminations must be initiated via help desk ticket for appropriate reviews, approvals, authorizations, and tracking.
- In addition, since the financial system has been identified as one of the district's critical systems, the review of access will be performed at least quarterly by one of the administrators in the district.
- The district will investigate whether notifications of access creation or modification can generate an automated notification that can be sent to other designated administrators.

These access management procedures shall be finalized and implemented no later than June 30, 2024.

4. Ensure that all officials and employees with access to PPSI receive annual data privacy and IT security and awareness training in accordance with District policy.

RESPONSE AND CORRECTIVE ACTION PLAN:

Copiague will ensure that all officials and employees throughout the district receive annual data privacy and IT security and awareness training in accordance with District policy.

Currently, we provide all officials and employees with online training annually, via [redacted] and have contracted with a third-party cybersecurity vendor that has provided onsite, live training for administrative staff and officials in January 2024.

In addition, the district has contracted with a third-party vendor application to perform periodic phishing tests throughout the year to continuously test and educate employees and officials of the dangers of phishing scams. Any employee or official that click on a phishing link will be required to take additional training.

These Security & Awareness Training procedures have been implemented as of January 1, 2024.

Submitted by:

Kathleen Bannon, 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. 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 interviewed District officials and employees and reviewed Board policies and regulations to gain an understanding of the District's policies and procedures related to nonstudent network and financial software access controls.
- We interviewed District officials to determine whether officials and employees received data privacy and IT security awareness training during the audit period.
- We examined enabled network user accounts as of October 19, 2022 using a computerized audit script. We analyzed the reports generated by the script and compared them to payroll records to determine whether all enabled nonstudent network user accounts were for current District employees. We analyzed the last logon dates for all user accounts to identify those not used within the last six months. We discussed the identified accounts with District officials to determine whether they were necessary and used by individuals currently employed by or working for the District.
- We used our professional judgement to select and examine the user access rights for 10 of the 67 user accounts with access to the financial software application to determine whether their access to the software was necessary and appropriate based on their job duties.

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. Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.ny.gov/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

https://www.osc.ny.gov/local-government

Local Government and School Accountability Help Line: (866) 321-8503

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