REPORT OF EXAMINATION | 2022M-121

Carle Place Union Free School District

Network User Account Controls

DECEMBER 2022

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

Contents

Report Highlights

Carle Place Union Free School District

Audit Objective

Determine whether Carle Place Union Free School District (District) officials established adequate controls over network user accounts.

Key Findings

District officials did not establish adequate controls over network user accounts. As a result, the District has an increased risk of unauthorized access to and use of its network and potential loss of important data. In addition to finding sensitive information technology (IT) control weaknesses that were confidentially communicated to officials, we found that District officials did not:

- Disable 52 unneeded employee network user accounts, 376 unneeded student network user accounts, 14 unneeded shared accounts and 25 unneeded service accounts.
- Establish written procedures for granting, verifying, changing and disabling network user account access.

Key Recommendations

- Establish written procedures for granting, verifying, changing and disabling network user account access.
- Disable network user accounts that are unneeded or have not been used after a specified period of inactivity.

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

Background

The District serves the Town of North Hempstead in Nassau County.

The District is governed by a five-member Board of Education (Board) that is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools 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 Director of Instructional Technology (Director) oversees the Office of Technology (IT office) and is responsible for establishing controls over District network user accounts. The District contracted with an outside vendor to provide two IT technicians who monitor and service the network under the Director's supervision.

Quick Facts

Enabled Network User Accounts	
Student	1,578
Employee	474
Service and Shared	67
Total	2,119

Audit Period

July 1, 2020 – February 9, 2022

Network User Account Controls

How Should Officials Establish Controls Over Network User Accounts?

Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access and loss. School district (district) officials should establish written procedures describing how staff should actively manage network user accounts – including their creation, use and dormancy – and regularly monitor them to ensure they are appropriate and authorized.

When network user accounts are no longer needed, they should be disabled in a timely manner. One way to accomplish this is to establish and implement a system in which user accounts are disabled after a reasonable specified period has elapsed without a valid user login. In addition, officials should regularly review enabled network user accounts to ensure they are still needed and disable unneeded accounts when they are no longer needed.

Officials should limit the number of enabled network administrative accounts and monitor them. A network administrative account has elevated permissions to make system-wide changes and monitor and control a network, computers connected to the network and certain applications. Network administrative accounts also can add new users and change users' passwords and permissions. These accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access a network and then view personal, private and sensitive information (PPSI),[1] make unauthorized changes to records or deny legitimate access to electronic information.

School districts should limit shared and service network user accounts because they are not linked to one individual. Therefore, managers may not be able to hold users accountable for their actions when using these accounts. Shared user accounts have usernames and passwords that are shared among two or more users. They often are used to provide access to guests or other temporary or intermittent users. IT staff use service accounts to run particular network or system services or applications (e.g., automated backup systems). District officials should routinely evaluate the need for these accounts and disable those that are not related to a current District or system need.

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

Officials Did Not Establish Adequate Controls Over Network User Accounts

District officials did not establish adequate controls over network user accounts for the District's network. They did not establish written procedures for granting, verifying, changing and disabling network user account access.

Unneeded Employee Network User Accounts – The Office of Instruction and Personnel (personnel office) forwards requests for network access to the IT office, and an IT technician creates network user accounts for the new employees. When an employee leaves District employment, the personnel office sends an interoffice memo (personnel action memo) to the Director asking him to disable the employee's network user account.

However, for substitute, seasonal or temporary (i.e., coaches) employees whose employment dates are determined when hired, the personnel office does not notify the IT office when the employees leave District employment. When these individuals are hired, the Board documents their beginning and ending employment dates in a resolution. The personnel office attaches the resolutions to a personnel action memo, which also documents these employees' employment end dates, and sends the memo to the Director.

We reviewed all 474 enabled employee network user accounts and found 52 that were unneeded because they were assigned to former employees. The accounts were active and unused since the employees left District employment, which ranged from August 2009 to June 2021. This means that these accounts were active and unused for anywhere from eight months to 12 years when the employees left District employment.

The IT technicians told us they did not disable the 52 unneeded accounts because the personnel office did not notify the IT office when the employees left District employment. However, the Assistant Superintendent for Instruction and Personnel (Assistant Superintendent) told us that the personnel office notified the IT office for 23 of the 52 former employees. The Assistant Superintendent provided us with copies of personnel action memos and Board resolutions that were sent to former Directors, notifying them that the 23 employees had left District employment and asking them to disable the former employees' network user accounts. However, this miscommunication demonstrates why officials should periodically review network user accounts to identify those that are unneeded.

For the remaining 29 former employees:

- 18 were substitute, seasonal or temporary employees. We reviewed two personnel action memos, with attached Board resolutions, and found that the employees' employment durations coincided with a specific school year or

the memos included a specific employment end date. Therefore, the IT office should have been aware of these employees' ending employment dates.

- The Assistant Superintendent could not locate the personnel action forms for four employees.
- Four unneeded user accounts were for teachers who were employees of the Nassau Board of Cooperative Educational Services (BOCES). The District contracted with the BOCES for remote teaching services provided by the four teachers during the summer of 2021. The Assistant Superintendent said that because this was a unique situation, there were no procedures in place to notify the IT office to disable these network user accounts.
- Two employees were hired as leave replacements. The Assistant Superintendent told us that leave-replacement appointments are often open-ended. For these employees, the Assistant Superintendent notified the principal or department head when the leave-replacement appointments ended, but she did not notify the IT office. The Assistant Superintendent told us that she intended to notify the IT office of ending leave-replacement appointments going forward.
- The IT office created one user account based on information provided in a draft August 20, 2020 Board agenda. The agenda indicated that a substitute teacher would be hired at the August 2020 Board meeting. However, the individual was not hired. Because the individual was never a District employee, the personnel office did not notify the IT office to disable the account.

The Director should document, evaluate and implement a system in which the personnel office notifies the IT office of new hires, retirements and employees who have left District employment only after the Board has approved them. If Board-approved appointments include an end date, the personnel office should communicate this to the IT office.

Also, the IT office should use this information to disable the user accounts of these individuals in a timely manner. In addition, IT technicians could set the network user accounts of employees who are appointed for a specified term to be automatically disabled on the users' last day of employment.

Unneeded Student Network User Accounts – Before the start of each school year, the District's central registrar emails a list of incoming kindergarten students to the IT office, and the IT technicians create network user accounts for the new students. The same procedure is followed when new students transfer into the District.

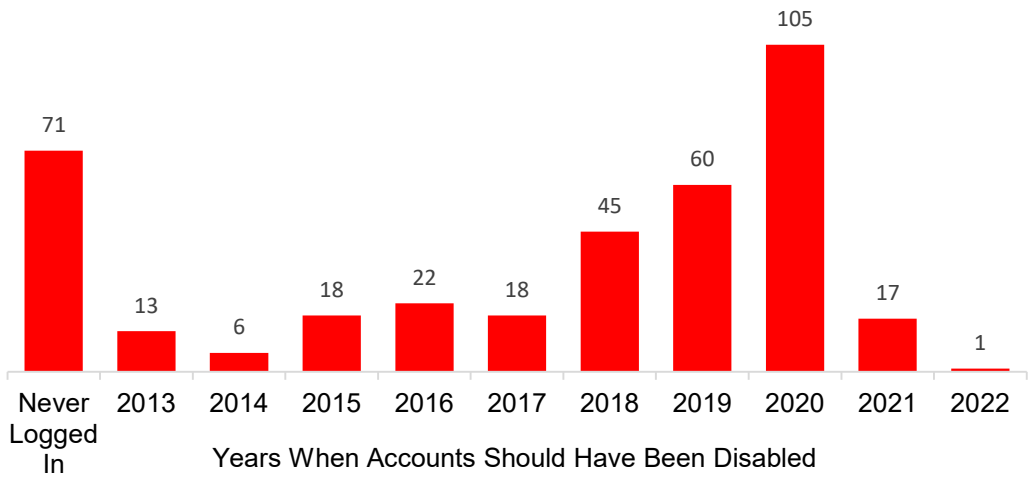
When high school students graduate, the IT technicians disable their network user accounts on the students' graduation day and permanently delete the accounts

two weeks later. However, the District did not have a procedure for notifying the IT office to disable a student network user account when a student leaves the District before graduating.

We reviewed all 1,578 enabled student network user accounts and identified 376 accounts (24 percent) that were unneeded because they were assigned to former students who left the District before graduating (Figure 1).

FIGURE 1

Former Student Accounts Not Used In At Least Six Months



The central registrar said that she did not notify the IT office when students left the District before graduating, because she thought their network user accounts would be automatically disabled when she disenrolled the students from the student information system.

Had the IT office periodically reviewed the accounts, IT staff would have identified and disabled the unneeded accounts without having to rely on notifications from other departments or individuals.

Unneeded Shared and Service Accounts – During our review of all 2,119 enabled network user accounts, we identified 15 shared user accounts and 52 service accounts. Of these 67 accounts, one shared user account and 27 service accounts had legitimate business purposes, but 14 shared accounts and 25 service accounts (39 total) were unneeded.

The IT technicians said they did not disable these accounts in a timely manner because the pandemic interrupted their normal routine (i.e., reviewing network user accounts during the summer months) and shifted their work priorities. They also said that working remotely during the height of the pandemic added to the delay.

However, we question if the procedures in place before the pandemic were appropriate because 12 of the 39 unneeded accounts were created before September 2019 and had never been used to log into the network. For example, two of the 12 accounts were created in April 2001 but had never been used to log into the network.

Also, another 12 of the 39 unneeded accounts were last used to log into the network before September 2019. The oldest two accounts (both created in March 2008) were last used to log into the network in August 2012 and July 2015. The remaining 15 accounts were either created, or last used to log into the network, after September 2019 but were no longer needed. If the previous procedures had been effective, 24 of the 39 accounts would have been disabled and would not have been included in our audit findings.

When an organization has unneeded network user accounts, this creates more difficulty for IT staff when managing and reviewing network access and user accounts. Also, unneeded network user accounts are additional entry points into the District's network. If an attacker accesses unneeded accounts, the attacker could use them to inappropriately access the District's network. An attacker could use these additional entry points to severely disrupt District operations by:

- Denying District employees access to information they need to perform their job duties.
- Installing malicious software that could cripple and/or completely shut down the District network.
- Obtaining and publicly releasing PPSI – such as employee and student date of birth, home address and social security numbers – which could be used to facilitate identity theft.
- Inappropriately accessing and changing District records, such as student grades.

These events would have criminal, civil, regulatory, financial, and reputational repercussions on District operations.

What Do We Recommend?

The Director should:

1. Develop and adhere to written procedures for granting, verifying, changing and disabling network user account access.

2. Disable network user accounts of former employees and students as soon as they leave District employment or enrollment and disable other unneeded user accounts in a timely manner.

3. Configure network user accounts to automatically disable network access of employees who have a specified employment term (e.g., seasonal employees and employees hired for annual appointments) after the users' specified last day of District employment.

4. Establish and implement a system in which network user accounts are disabled after a specified period of inactivity.

5. Evaluate all current network user accounts and disable those that are unneeded. Also, establish and implement a system to periodically review network user accounts to determine whether they are needed, and promptly disable those that are deemed unneeded.

The Assistant Superintendent should:

6. Promptly notify the IT office of starting and ending employment dates for substitute, seasonal and temporary employees. Also, promptly notify the IT office when employees retire and otherwise leave District employment.

The central registrar should:

7. Promptly notify the IT office when students leave the District before graduating.

Appendix A: Response From District Officials

Carle Place Union Free School District

168 Cherry Lane
Carle Place, New York 11514-1788

November 2, 2022

STATE OF NEW YORK OFFICE OF THE STATE COMPTROLLER
Hauppauge Regional Office
250 Veterans Memorial Highway
Room 3A10
Hauppauge, NY 11788

To Whom It May Concern:

The Carle Place Union Free School District is in receipt of the draft Report of Examination regarding its Network User Accounts for the audit period July 1, 2020 through February 9, 2022. Please accept this letter as the District's response to the draft Report.

The District and its Board of Education takes their obligations to maintain security of the District's computer network very seriously. In this regard, we note that the District has multiple layers of security protection in place, including a firewall, intrusion detection systems, web filtering, DNS (Domain Name System) filtering and anti-virus scanning. We would also like to acknowledge the strength of our IT department which, while maintaining day-to-day operations, also supported remote learning for students, staff, and parents during the pandemic.

We acknowledge the findings and recommendations set forth in the draft Report. The Board of Education and Central Office Administration view such findings and recommendations as an opportunity to continue our ongoing efforts to improve governance and operations within the District. We will prepare our Corrective Action Plan and will submit upon review and approval by the Board of Education.

The District has already complied with the recommendation to disable all network user accounts identified as unneeded. As always, the District will continue to implement policies and procedures that provide users, employees, and the school community a safe, sound, and beneficial educational IT environment.

The District appreciates the time and effort undertaken by the representatives of the Office of the State Comptroller and would like to take this opportunity to thank them for their professionalism throughout the audit process.

Sincerely,

[redacted]

Dr. Christine Finn
Superintendent of Schools

Cc: Board of Education
Joanna DeMartino, Assistant Superintendent for Business

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed the Assistant Superintendent, central registrar, Director and both IT technicians to gain an understanding of the District's network user account controls, specifically those related to granting, verifying, changing and disabling network user account access.
- We examined network user accounts, including their permissions, using a computerized audit script run on February 9, 2022. We reviewed all enabled network user accounts and compared them to current employee and student lists to identify unused and possibly unneeded network user accounts.
- We interviewed the Director and both IT technicians to discuss possibly unneeded network user accounts.
- We interviewed the Assistant Superintendent to determine why the District had active unneeded employee network user accounts and the central registrar to determine why the District had active unneeded student network user accounts.

Our audit also examined the adequacy of certain sensitive 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.state.ny.us/files/local-government/pdf/regional-directory.pdf

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

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

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

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

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

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

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

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

Contact

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

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

www.osc.state.ny.us/local-government

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller