New York State Comptroller
THOMAS P. DiNAPOLI

Brentwood Union Free School District

Information Technology

2023M-83 | November 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Brentwood Union Free School District

Audit Objective

Determine whether the Brentwood Union Free School District (District) Board of Education (Board) and officials ensured computerized data was safeguarded by monitoring network user accounts, providing network users with information technology (IT) security awareness training and implementing an IT contingency plan.

Key Findings

The Board and District officials did not adequately monitor nonstudent network user accounts, provide IT security awareness training as required by a Board-adopted policy or implement an IT contingency plan.

As a result, the District's computerized data was not adequately safeguarded. In addition, the District has an increased risk that the network may be accessed by unauthorized individuals, data will be lost and the District may not be able to recover from a network disruption or disaster.

In addition to sensitive IT control weaknesses that we communicated confidentially to District officials, we also found that officials did not:

- Disable 486 of the 3,525 enabled nonstudent network user accounts (14 percent) that we reviewed and determined were not needed.
- Establish written procedures for granting, changing and disabling network user account access.

Key Recommendations

- Periodically review network user accounts and disable accounts that are not needed.
- Provide the Board-required IT security awareness training.
- Develop a comprehensive IT contingency plan.

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

Background

The District serves the Town of Islip in Suffolk County. The elected seven-member Board is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer and is responsible, along with other administrative staff, for District's day-to-day management under the Board.

The IT Coordinator is responsible for managing the District's IT operations, including the IT department with 14 employees across 22 District buildings, and ensuring computerized data is properly safeguarded by monitoring nonstudent network user accounts.

Quick Facts	
Student Enrollment	17,608
Employees	2,030
Network User Accounts	
Student	20,399
Nonstudent	3,525
Total	**23,924**

Audit Period

July 1, 2021 – October 18, 2022

Information Technology

How Should Officials Manage and Monitor Network User Accounts?

An individual network user account has a unique username and password and is designed to only be used by the assigned user. To help minimize the risk of unauthorized network access and safeguard computerized data, the IT Coordinator and IT department staff should actively manage and monitor network user accounts by periodically comparing the list of current active employees and current vendors to the list of network user accounts to determine if user accounts belong to current employees and vendors. Any account that cannot be associated with a current authorized user or school district need should be disabled immediately, when user account access is no longer needed. IT officials should have written procedures in place to grant, change and disable user account access to the network in a timely manner (e.g., upon an employee leaving employment at the school district). Disabling accounts in a timely manner is important because depending on a user's job duties and responsibilities, the account may have access to personal, private and sensitive information (PPSI). 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, students, third parties or other individuals or entities.

Officials should also limit the use of shared and service network user accounts, as they are not linked to one individual and school district officials may have difficulty linking any suspicious activity to a specific user. School district officials should routinely monitor and evaluate the need for the accounts and disable those that are not related to a current district or system need. 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 Did Not Adequately Manage and Monitor Network User Accounts

IT department staff, including the IT Coordinator, did not adequately manage and monitor nonstudent network user accounts we reviewed. Network user accounts were not disabled as soon as they were no longer needed. In addition, they did not periodically compare a list of current active employees and vendors to a list of enabled network user accounts to identify and disable unneeded accounts. IT department staff also did not routinely evaluate the need for shared and service network accounts. As a result, the District had unneeded network user accounts that were not disabled.

This occurred because the District did not have written procedures to disable network user account access when employees and service providers separated

from the District and the IT Coordinator did not periodically review all enabled network user accounts for necessity and appropriate access. The IT Coordinator could not explain why the District did not have written procedures for granting, changing and disabling nonstudent user account access to the network.

We ran a computerized audit script in October 2022 and determined that the District had 3,525 enabled nonstudent network user accounts, including 2,934 individual network user accounts and 591 shared and service network user accounts. Working with District officials, we determined that 486 nonstudent network user accounts (14 percent) were not needed and should have been disabled.

Individual Network User Accounts – We reviewed all 2,934 individual nonstudent network user accounts and, working with officials, determined that 131 individual user accounts (over 4 percent) were not needed and should have been disabled, including:

- 93 user accounts assigned to former District employees. These enabled user accounts included three user accounts assigned to former employees who separated from the District more than 12 years ago, and eight user accounts assigned to former teachers that remained enabled for an average of four years after they left employment. In addition, these eight user accounts were logged into after the teachers separated from the District. The IT Coordinator could not explain why these accounts were logged into after the teachers separated from the District but said these user accounts were disabled as a result of our audit inquiry. When network user accounts are not disabled in a timely manner at separation, there is an increased risk that student data and other District applications and systems such as email could be inappropriately accessed and possibly used for malicious activity.
- 34 user accounts assigned to former service providers that no longer provided services to the District. These user accounts included four that were not used in as much as five years and one that was not used in 14 years.
- Two user accounts assigned to former Board trustees that remained enabled four months after they were no longer on the Board. The two accounts were set to expire at the end of the trustees' term; however, they were not disabled until after our inquiry.
- Two user accounts that were last used in July 2020 and January 2022. The IT Coordinator could not explain the business purpose for the accounts and disabled them after our inquiry.

The IT Coordinator stated that individual network user accounts were not disabled in a timely manner because the District did not have consistent procedures when individuals separated from or stopped providing service to the District. These individual network user accounts should have been disabled when the users

separated from or stopped providing services to the District. Because these network user accounts were not disabled, they could have been used by those individuals or others for malicious purposes.

Shared and Service Network User Accounts – We determined that 425 (72 percent) of the 591 shared and service network user accounts reviewed were not used to log in to the network in at least six months, including three user accounts that last logged in to the network in 2006. The IT Coordinator reviewed these 425 shared and service user accounts and indicated that 295 accounts were unnecessary and should be disabled, including 46 of these accounts that had never been used to log in to the network. The IT Coordinator identified that an additional 60 recently used or created shared and service network user accounts were also unnecessary and should have already been disabled.

The shared network user accounts were created for various purposes, including temporary and guest accounts and service accounts were for software programs used by District officials. IT officials did not have procedures to routinely review accounts to determine whether any were unnecessary and should be disabled. The IT Coordinator could not explain why these shared and service network user accounts had not been disabled. While the IT Coordinator provided a list showing that 29 of the accounts were temporary shared accounts set with an expiration date, the accounts expired an average of 85 days after the last date the account logged in to the network instead of being disabled immediately when no longer needed.

Unneeded network user accounts are additional entry points into a network and, if compromised by an attacker, could be used to view and/or remove personal information accessible by that compromised network account; make unauthorized changes to official District records; or deny legitimate access to the District network and records. An attacker could use these additional entry points to 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's network.
- Obtaining and publicly releasing PPSI. For example, employee and student dates of birth and home addresses are considered PPSI and could be used to facilitate identity theft.

When a network is compromised, it could have criminal, civil, regulatory, financial and reputational impacts on District operations. Additionally, when a school district has many enabled network user accounts that must be managed and reviewed, it could make unneeded account detection less timely and accounts could be inadvertently granted unneeded permissions. During our fieldwork, the

IT Coordinator told us she conducted a thorough review of all enabled nonstudent network accounts and disabled all unneeded network user accounts that were identified as a result of our inquiry.

Why Should Officials Provide IT Security Awareness Training?

Studies show that human error accounts for a significant share of all cybersecurity breaches. Therefore, to safeguard computerized data and help minimize the risk of unauthorized access and misuse or loss of data and PPSI, school district officials should ensure periodic 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 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. Training programs should be directed at the specific audience (i.e., system users or administrators).

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 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 Employees Were Not Provided IT Security Awareness Training

The Board adopted a policy stating the District will provide annual IT security awareness training to all employees who have access to student and teacher PPSI. However, the Board and District officials did not enforce the policy and provide IT security awareness training to help ensure employees understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the District's network and IT assets. The Assistant Superintendent for Business and IT Coordinator said that IT security awareness training was not provided due to the limited time available for employees to take professional development and training courses during work hours. The IT Coordinator said she sends out monthly emails to all District staff that address emerging trends in IT security. However, because there is no certainty that recipients are reading these emails, this was not the most effective way to provide IT security awareness to employees. As a result of our audit, the IT Coordinator said the District plans to start providing IT security awareness training annually in the same manner that other required trainings are offered.

Without periodic comprehensive IT security awareness training, network users may not understand their responsibilities to safeguard computerized data and are more likely to be unaware of a situation that could compromise the District's IT assets and security.

Why Should the Board and District Officials Develop and Adopt an IT Contingency Plan?

A school district board and officials should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of computerized data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. These events can include power outages, software or hardware failures caused by a virus or other type of malicious software (e.g., ransomware), human error, equipment destruction or a natural disaster (e.g., flood, fire).

To develop an IT contingency plan, officials should analyze business processes and continuity needs, identify roles of key individuals and necessary precautions to recover data and quickly resume operations in the event of an unplanned disruption. Officials should ensure the IT contingency plan also includes data back-up procedures, such as ensuring backups are stored off-site and off-network and requiring IT staff to periodically test backups to ensure they will function as expected.

School district officials should periodically test and update the plan, as needed, to help ensure officials understand their roles and responsibilities during and after a disruptive event. Testing and updating IT contingency plans are particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks. These plans should be distributed to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements.

The Board and District Officials Did Not Develop and Adopt an IT Contingency Plan

The Board and District officials did not develop and adopt an IT contingency plan to document and inform staff how they should respond to unplanned disruptions and disasters that affect the District's IT environment. The IT Coordinator stated that back-ups are routinely performed and tested, but due to limited IT staffing resources, an IT contingency plan had not been developed.

Without a comprehensive IT contingency plan, District officials cannot guarantee that in the event of a disruption or disaster, such as a ransomware attack, employees would be able to help resume, restore, repair and/or rebuild critical IT systems, applications or data in a timely manner. Depending on the severity of an

incident, officials may need to expend significant time and financial resources to resume District operations. Furthermore, responsible parties may not be aware of their roles, complicating the District's ability to recover from an incident. As a result, important financial and other data could be lost, or the District could suffer a disruption to operations that depend on its computerized environment.

What Do We Recommend?

The Board and District officials should:

1. Ensure users are annually trained in IT security awareness issues and the proper usage of the Internet and IT systems and data in accordance with the Board-adopted policy.

2. Develop and adopt a comprehensive IT contingency plan that provides specific guidelines for the protection of IT assets and data, including the network and financial application, against loss or destruction.

District officials and the IT Coordinator should:

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

4. Ensure that unnecessary network user accounts are disabled in a timely manner and periodically review network user accounts for necessity and appropriateness of access.

Appendix A: Response From District Officials

TBD
Interim Assistant Superintendent of
Secondary Education
631-434-2498
631-434-2115

Stacy O'Connor
Assistant Superintendent for
Finance & Operations
631-434-2311
Fax: 631-434-3104

Brentwood Union Free School District

Wanda Ortiz-Rivera
Interim Superintendent of Schools
631-434-2325
Fax: 631-273-6575

Ann Palmer
Assistant Superintendent for
Elementary Education
631-434-2496

Rhonda Young
Assistant Superintendent of
Special Services
631-434-2143

October 24, 2023

Mr. Ira McCracken
Chief of Municipal Audits
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, NY 11788

Dear Mr. McCracken:

The District confirms it is in receipt of the draft Review of Information Technology for the period of July 1, 2021, to October 18, 2022. On behalf of the Board of Education and the District's administrative team, we extend our appreciation for the valuable insights provided by the Comptroller's Office.

Our District is committed to providing an exceptional educational experience to all our students. We welcome the opportunity to further enhance our practices and protocols. The audit conducted by your office placed its focus on three critical aspects: the safeguarding of network user accounts, the implementation of cybersecurity awareness training, and the establishment of an IT contingency plan.

In response to the findings and recommendations highlighted in the review, the District is undertaking or is in the process of the following actions:

1. The disabling of all unnecessary network accounts while the Comptroller's staff was onsite.
2. The initiation of the process of formulating a comprehensive cybersecurity training program.
3. The development of an IT contingency plan.

We extend our gratitude to the Comptroller's Office for their time and effort invested in this audit. Please rest assured that the District is fully committed to addressing and accomplishing the tasks outlined above, as we are determined to fortify our IT systems and uphold the highest standards of cybersecurity.

Sincerely,

Wanda Ortiz-Rivera
Interim 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. 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 District officials to gain an understanding of the District's IT operations, specifically focusing on those relating to how officials ensure District computerized data was safeguarded, including the monitoring of nonstudent network user accounts, the existence of an IT contingency plan and whether any employees received IT security awareness training and determine the adequacy of the policies and procedures.
- We examined network user accounts on the District's domain controller as of October 18, 2022 using a computerized audit script that identified 23,924 enabled network user accounts. We determined that 20,399 of those accounts were student-related accounts and assigned to a student domain. The student domain accounts are granted limited access to the network and have limited risk associated with them; therefore, we did not include them in our audit objective and testing. For the remaining 3,525 network accounts, we compared the District's employee master list to the enabled network user accounts identified by the script to determine whether enabled network accounts were associated with District employees or third parties, or if they were shared or service accounts.
- We reviewed the last login date for network user accounts to identify unused and possibly unneeded network user accounts and followed up with the IT Coordinator to determine whether the user accounts were appropriate and needed.

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.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 11788-5533

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

Serving: Nassau, Suffolk counties