New York State Comptroller
THOMAS P. DiNAPOLI

# East Hampton Union Free School District

## Network and Financial Application Access and Information Technology Contingency Planning

**2023M-8 | September 2023**

**Division of Local Government and School Accountability**

# Contents

# Report Highlights

**East Hampton Union Free School District**

## Audit Objective

Determine whether East Hampton Union Free School District (District) officials secured user account access to the network and financial application and developed an information technology (IT) contingency plan.

## Key Findings

District officials secured user account access to the financial application but did not secure user account access to the network or develop an IT contingency plan. This increases the risk of unauthorized access, lost data, and inability to recover from a network disruption. We confidentially communicated sensitive IT weaknesses to officials, and also determined:

- The District's use of two central network management tools for over 10 years has created security concerns due to lack of monitoring of all accounts on both tools.
- Ninety-one percent, or 3,395, of the District's enabled network user accounts were not logged into in the last six months. Accounts grant access to sensitive information, and unneeded accounts should be disabled to protect District data.
- Officials did not provide IT security awareness training to District IT users. Therefore, users may not understand their responsibilities and are more likely to be unaware of situations that could compromise the District's IT network and data.

## Key Recommendations

- Disable unnecessary network user accounts and periodically review them for necessity.
- Provide periodic IT security awareness training to all District IT users.
- Develop and adopt a comprehensive written IT contingency plan.

District officials disagreed with certain findings in our report but indicated that they will initiate corrective action. Appendix B includes our comments on certain issues officials raised in their response.

## Background

The District is located in the Town of East Hampton in Suffolk County and operates three schools.

The District is governed by an elected seven-member Board of Education (Board) responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the 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 Network and Systems Administrator (Systems Administrator) is responsible for setting up users within the financial application and for managing the District's IT network, including securing user account access to the network.

| Quick Facts | |
|---|---|
| Student Enrollment | 1,832 |
| Employees | 221 |
| **Enabled Network User Accounts** | |
| Student | 3,132 |
| Individual Nonstudent | 483 |
| Shared and Service | 110 |
| Total | 3,725 |

## Audit Period

July 1, 2021 – October 17, 2022

# Network and Financial Application Access and IT Contingency Planning

A school district relies on its network, financial application and other IT assets for maintaining financial, student and personnel records, and Internet access and email, much of which contain personal, private and sensitive information (PPSI). PPSI is any information to which unauthorized access, disclosure, modification, destruction – 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. The District has been using two different central network management tools for over 10 years.

## How Should School District Officials Secure User Account Access to the Network and Financial Application?

School district officials should timely disable any account that cannot be associated with a current authorized user or school district need, and periodically conduct a user account review to identify and disable any accounts that are no longer needed. School district officials should actively manage network and financial application user accounts to minimize the risk of unauthorized network and financial application access.

School district officials should have written procedures in place for granting, changing and disabling user account access to the network and financial application. These procedures should establish who has the authority to grant or change user account access.

School district officials should have written procedures in place for granting, changing and disabling user account access to the network and financial application.

Shared and service network user accounts should be limited in use, as they are not linked to one individual and, therefore, may have reduced accountability. School district officials may have difficulty managing the accounts and linking any suspicious activity to a specific user. A shared user account has a username and password that is shared among two or more people and can be 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). School district officials should routinely evaluate the need for the accounts and disable those that are not related to a current district or system need.

## District Officials Did Not Adequately Secure User Account Access to the Network

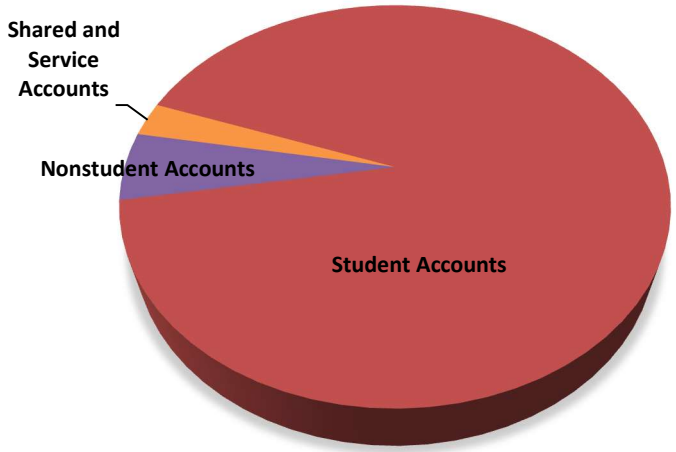
Although the Systems Administrator adequately secured user account access to the District's financial application, he did not adequately secure user account access to the network.

We reviewed all 3,725 enabled network user accounts, including 3,132 student accounts, 483 individual nonstudent accounts and 110 shared and service accounts. We identified 3,395 (91 percent) network user accounts that were not

used to log into the network for at least six months, most of which should have been disabled (Figure 1). The Systems Administrator explained that, since the District has begun migrating to its current central network management tool, officials have not gone back to disable unnecessary network user accounts in the existing central network management tool. However, the migration has been ongoing since 2013 and accounts still grant access to sensitive information. Therefore, officials should be reviewing the District's original central network management tool for unnecessary network user accounts and disabling or deleting any accounts that have not been used to log into the network for at least six months.

**FIGURE 1**

**Unneeded Network User Accounts**




Student and Individual Nonstudent Accounts – We identified 3,302 enabled network user accounts (89 percent), including 3,117 student accounts and 185 individual nonstudent accounts, that had not been used to log into the network in over six months. Upon further review and discussion with the Systems Administrator, we determined that, while the District did have written procedures for disabling network user account access, the Systems Administrator did not do so and, as a result, none of the student (3,117) and individual nonstudent (185) network user accounts were detected as unnecessary and disabled as they should have been. Furthermore, we identified 104 student accounts and three individual nonstudent accounts that had not been used in over 10 years. When we discussed these accounts with the Systems Administrator, he stated that he would be keeping a limited number of network user accounts enabled on the existing central network management tool. These include accounts for various programs that are not compatible with the new tool, such as certain lab programs. However, the Systems Administrator did not specify how many accounts would be kept enabled on the existing central network management tool.

Shared and Service Network User Accounts – We identified 93 shared and service network user accounts that had not been used to log into the network in over six months. Furthermore, there were 18 shared and service network user accounts that had not been used in over 10 years. These shared and service network user accounts were created for various purposes, including backup third-

party user account access, an adult education program and email support. Based on our discussion with the Systems Administrator, we determined that 64 shared and service network user accounts were no longer needed and should have been disabled. During our discussion with him on October 13, 2022, the Systems Administrator disabled these 64 accounts, as well as another 11 shared and service network user accounts that he identified as unneeded as a result of our audit inquiry. The Systems Administrator told us he had not previously disabled these accounts because he was focusing his attention on the migration. However, the Systems Administrator should still have been reviewing the user accounts enabled on the existing central management tool to disable or delete unnecessary accounts.

Unused and unneeded network user accounts are additional entry points into the District's network and, if compromised by an attacker, could be used to inappropriately access the District's network and then review and/or remove personal information; make unauthorized changes to official District records; or deny legitimate access to the District's network and records. An attacker could use these additional entry points to severely disrupt District operations by:

- Denying District employees network access to electronic information they need to perform their job duties, such as student medical records or individual education programs, and
- Installing malicious software that could cripple and/or completely shut down the District's network by accessing an account with administrative permissions, such as a shared or service account.

When a school district has many network user accounts that are not adequately managed and reviewed, unneeded network user accounts increase the risk of unauthorized access by users, possibly with malicious intent. During the migration, the District has been limiting the user accounts to teaching, staff and administrative users, as needed, based on their job duties. Even though the user accounts will be limited, there still remains the risk of unauthorized access by users.

Further, District officials indicated in their response to the audit that they do not have a planned end of life for their original network management system, and that both systems are expected to operate in parallel indefinitely. This makes the risk associated with the audit's findings even more consequential than if this had been a planned "migration," as the Systems Administrator asserted during our audit. With no expected end-of-life date for the original system, it is critical that the security configurations of that system are actively managed to align with industry best practices.

Because the District is using the original system to manage users and devices that have access to financial software, and due to the high-value nature of that

data, the users and devices with access to this software are at a higher risk of compromise. They should, therefore, be actively managed at a higher level of security, rather than a lower one.

### Why Should School District Officials Provide IT Security Awareness Training?

School district officials should provide periodic comprehensive IT security awareness training to help minimize the risk of unauthorized access to the network and financial application and the misuse or loss of the data and PPSI therein. IT security awareness training should explain rules of behavior for using the Internet and the District's financial application and the network, and communicate related policies and procedures to all District IT users. The training should center on, but not be limited to, emerging trends such as information theft, social engineering attacks (methods used to deceive users into revealing confidential or sensitive information), and computer viruses and other types of malicious software, all of which may result in PPSI compromise or denying access to the District's financial application and the network. Training programs should be directed at the specific audience (e.g., system users or administrators).

The training should also cover key security concepts such as the dangers of browsing and downloading files and programs from the Internet; the importance of selecting strong passwords; requirements related to protecting PPSI; and how to respond if a virus or an information security breach is detected. To ensure officials are aware they need to provide IT security awareness training, the board should adopt a policy and implement written procedures requiring IT security awareness training.

### Officials Did Not Provide IT Security Awareness Training

District officials did not provide users with IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the District's network and IT assets. In addition, the District does not have a Board-adopted policy or written procedures in place requiring IT security awareness training. Without having training, staff may be more likely to open malicious emails, putting the District at risk of viruses or social engineering attacks. The Systems Administrator could not explain why the District did not provide IT security awareness training, as it is a foundational IT concept and training resources are available at no cost to the District.

Without periodic comprehensive IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise the District's IT network and data. As a result, data and PPSI are at a greater risk for unauthorized access, misuse or loss.

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

## Why Should the District Have an IT Contingency Plan?

The board and district officials should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. An IT contingency plan is a district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT disruption or disaster. The plan should address the potential for sudden, unplanned disruptions (e.g., system failure caused by inadvertent employee action, power outage, ransomware or other type of malware infection, or a natural disaster such as a flood or fire) that could compromise the network and the availability or integrity of the school district's IT system and data, including its financial application and PPSI contained therein.

Typically, IT contingency planning involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to maintain or quickly resume, restore, repair and/or rebuild operations. The plan should be periodically tested, updated as needed and distributed to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes, such as statutory changes.

## Officials Did Not Have an IT Contingency Plan

The Board and District officials did not adopt an IT contingency plan to describe how officials should respond to potential unplanned IT disruptions and disasters affecting the District's operations that depend on its IT environment. The Board and District officials have been developing an IT contingency plan; however, according to the Systems Administrator, the Board has not yet adopted the plan because the Board and District officials have been unable to agree on wording.

Without a contingency plan, officials have less assurance that, in the event of a disruption or disaster such as a ransomware attack, employees and other responsible parties would be able to react quickly and effectively 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, the District has an increased risk that it could lose important data and suffer a serious interruption in operations that depend on its computerized environment, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims.

## What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a policy and written procedures for providing IT security awareness training.

2. Develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

District officials and the Systems Administrator should:

3. Disable unnecessary network user accounts, including those in the existing central network management tool, in a timely manner, and periodically review network user accounts for necessity and appropriateness.

4. Ensure that users receive periodic comprehensive IT security awareness training that includes current risks identified by the IT community.

# Appendix A: Response From District Officials

**EAST HAMPTON UNION FREE SCHOOL DISTRICT**
**4 LONG LANE**
**EAST HAMPTON, NY 11937**



August 7, 2023

Thomas P. DiNapoli
New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor
Albany, NY 12236

**Re: NYS Audit/Plan Response**

Dear Comptroller DiNapoli:

I write on behalf of the Board of Education of the East Hampton Union Free School District to acknowledge receipt of your office's recent audit of the District, *Network and Financial Application Access and Information Technology Contingency Planning, 2023M-8.*

I would like to thank you for your office's review of our operation and the thoroughness and professionalism of the auditors who were here to conduct the review.

I appreciate the three key findings of your audit, and I wish to respond briefly to each point.

First, we agree with your finding that we are running two central network management tools over the last 10 years. However, I respectfully disagree with the characterization of this practice as a "migration". We have purposefully moved to the [redacted] suite for a number of our applications but we are required to maintain the [redacted] suite for certain programs and applications that are not compatible with the [redacted] package. For example, the [redacted] financial software does not run on [redacted], nor does [redacted] a screen annotation and teaching tool for interactive whiteboards and displays. Should these programs ever become [redacted]-compatible, we anticipate discontinuing support of the [redacted] platform.

See Note 1 Page 10

Second, we understand your impression that we have 3,395 enabled network user accounts. However, it should be noted that these accounts are disabled and inaccessible to anyone but the system administrator. These accounts, which were formerly assigned to students

See Note 2 Page 10

Superintendent of Schools 631-329-4104 Fax: 631-324-0109 | Assistant Superintendent 631-329-4133 Fax: 631-324-0109 | District Office 631-329-4100 Fax:631-324-0109 | Business Office 631-329-4106 Fax: 631-329-7550

and staff who have subsequently left the District, are preserved for archival purposes. This allows us to access the work product of past staff and allows former students to request copies of work they accomplished during their time here.

Third, we agree that IT security awareness training needs improvement. The District has been passively testing our employees with simulated phishing e-mails in attempts to ascertain which employees need additional security awareness training. At your suggestion, we will be instituting an annual IT security training program for all employees.

The Board of Education and I welcome audits in the East Hampton Union Free School District as we are seeking continuous improvement in our operation. I am very proud of what we have here in the District and I am eager to use your audit as a guide to achieve even better operations.

Sincerely,

Adam S. Fine
Superintendent of Schools

ASF:kss
cc: Timothy B. Fromm, Assistant Superintendent
Sam M. Schneider, Assistant Superintendent for Business
Charles Westergard, Network and Systems Administrator

# Appendix B: OSC Comments on the District's Response

Note 1

We updated the report based on information District officials provided in their response. In addition, the audit finding is not that the District was running two central network management tools, but that officials were not reviewing the user accounts and disabling or deleting unnecessary user accounts in the District's original network management tool.

Note 2

While District officials' audit response indicates these accounts were disabled, they were enabled when we conducted our audit work and when discussed the accounts with the Systems Administrator.

# Appendix C: 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 Superintendent, Assistant Superintendent for Business and the Systems Administrator to gain an understanding of the IT environment and determine whether:
  - Officials secured user account access to the District's network and financial application,
  - IT security awareness training was periodically provided, and
  - The District had an IT contingency plan.
- We ran the audit scripts on August 3, 2022 and, from those results, we reviewed the last login dates for network user accounts to identify unused and possibly unneeded network user accounts. We followed up with the Systems Administrator to determine whether the user accounts were appropriate and needed.
- We interviewed the Systems Administrator and reviewed software permissions reports from the financial application provided by the Systems Administrator on July 27, 2022, to determine how application user account access was secured. We examined the permissions granted to accounts associated with all six business office employees and one high school administrator to determine whether the Systems Administrator had adequately secured access to the financial application. We also reviewed the application user account permissions for these employees to determine whether they were appropriate based on their job duties.
- We reviewed the District's external audit management letters to determine whether officials were advised of any outstanding IT issues at the District.

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 D: 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