New York State Comptroller
THOMAS P. DiNAPOLI

# Montauk Union Free School District

## Information Technology

**2022M-137 | January 2023**

**Division of Local Government and School Accountability**

# Contents

# Report Highlights

**Montauk Union Free School District**

## Audit Objective

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

## Key Findings

Although District officials restricted access to the financial application, they did not adequately secure access to the network or develop an IT contingency plan. As a result, there is 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 were confidentially communicated to officials, we found:

- Twenty-five percent, or 140, of the District's network user accounts were not needed.
- Two unknown individuals had an active network user account.
- IT security awareness training was not provided.

Since 2013-14, external auditors have annually recommended that the District develop an IT contingency plan. However, the District never developed the plan and could not provide a reasonable explanation for failing to do so.

## Key Recommendations

- Periodically review network user accounts and disable any unnecessary accounts as soon as they are no longer needed.
- Provide periodic IT security awareness training.
- Develop and adopt a comprehensive written IT contingency plan.

District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

## Background

The District is located in the Town of East Hampton in Suffolk County and operates one school (prekindergarten through eighth grade).

The District is governed by an elected five-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 Treasurer is responsible for managing the District's financial operations and setting up users within the financial application. One of the District's teachers is responsible for managing the District's IT systems and assets (IT Director).

| Quick Facts | |
|---|---|
| Student Enrollment | 338 |
| Employees | 61 |
| **Network User Accounts** | |
| Student | 393 |
| Non-Student | 115 |
| Other | 44 |
| Total | 552 |

## Audit Period

July 1, 2020 – July 15, 2022

# Network and Financial Application Access

A school district relies on its network 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 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.

Unneeded network user accounts should be disabled in a timely manner.

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

To minimize the risk of unauthorized network and application access, school district officials should actively manage network and financial application user accounts and periodically conduct a user account review. Any account that cannot be associated with a current authorized user or school district need should be disabled.

School district officials should have written procedures in place to grant, change and disable user access to the network and financial application. These procedures should establish who has the authority to grant or change user access. Unneeded network user accounts should be disabled in a timely manner.

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 people 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). School district officials should limit the use of shared and service accounts and 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 Access to the Network

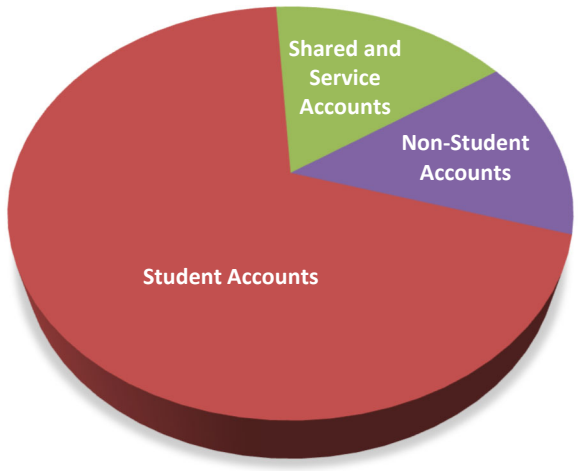
Although the IT Director and Treasurer adequately restricted access to the District's financial application, they did not adequately secure user account access to the network.

We reviewed all 552 enabled network user accounts, including 393 student accounts, 115 non-student accounts and 44 shared and service accounts. We found 140 network user accounts that were not needed for as much as 10 years and should have been disabled (Figure 1). The IT Director could not explain why the District does not have written procedures for granting, changing and disabling user account access to the network.

Student and Non-Student Accounts – We identified 137 network user accounts (27 percent), including 97 student accounts and 40 non-student accounts, that had not been used for as much as nine years; 30 of these accounts were never used. The IT Director did not provide an explanation as to why the 97 student network user accounts were inactive and had not been disabled. After the exit conference we inquired again and the IT Director informed us that approximately half the 97 user accounts were for students enrolled in the District at the time of our audit test, but he did not clarify whether any of the 97 accounts were necessary.

**FIGURE 1**

**Unneeded Network User Accounts**




Additionally, 20 non-student network user accounts were unnecessary and should have been disabled, including 13 assigned to former employees. For example, a former substitute teacher had an enabled network user account for more than one year after separation and a former Board member still had an enabled network user account. District officials could not identify the assigned user for two non-student network user accounts, one of which had not been used since March 2013 and the other since September 2020. The IT Director could not explain why these accounts had not been identified as unneeded and disabled.

Shared and Service Network User Accounts – We identified 33 shared and service network user accounts that had not been used for as much as 10 years; 19 of these accounts had never been used. These shared and service network user accounts were created for various purposes, including a backup third-party account, network user accounts for students to share and accounts used to access servers. Based on our discussion with the IT Director, we determined that 23 shared and service network user accounts were no longer needed and should have been disabled, including service and template accounts.[1] While the IT Director is responsible for maintaining these accounts, he could not provide a reason why these accounts had not been disabled.

1 Template accounts are in use for student account creation, but they are never logged into. New student accounts are created by copying from the template account to ensure they have the correct account configuration.

The IT Director informed us after our audit fieldwork was completed that he conducted a thorough review of all enabled network accounts and disabled all unneeded network user accounts.

Unused and unneeded network user accounts are additional entry points into the District's network and, if accessed by an attacker or a former employee or student, could be used to inappropriately access the District's network to review and/or remove personal information; make unauthorized changes to 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 individualized education programs;
- Installing malicious software that could cripple and/or completely shut down the District's network by accessing a service account with administrative permissions;
- Obtaining and publicly releasing PPSI, such as employee and student dates of birth, home addresses and social security numbers, that could be used to facilitate identity theft;
- Removing and publicly releasing sensitive information related to District operations, such as personnel action reports and other confidential District Board matters that the Board would discuss during the executive session of a Board meeting; and
- Inappropriately accessing and changing District records, such as student grades.

When a school district has many network user accounts that must be managed and reviewed, unneeded network user accounts increase the risk of inappropriate access by users with malicious intent.

## Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access to the network and financial application, and misuse or loss of data and PPSI, school district officials should provide periodic IT security awareness training that explains rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all users. The training could 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), computer viruses and other types of malicious software, all of which may result in PPSI compromise or denying access to the IT system and its data. 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.

A board and school district officials should establish a policy and written procedures that require users to be trained in IT security awareness issues and in the usage of the IT infrastructure, software and data. While an IT security awareness policy and procedures will not guarantee the safety of the district's systems, without an adequate policy and procedures to require and provide training that explicitly conveys the appropriate use of a district's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

## 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. The IT Director could not explain why the District did not provide IT security awareness training, as it is a foundational IT concept and resources are available at no cost to the District. The IT Director said that the District plans on starting this training as a result of our audit.

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 assets and security. As a result, data and PPSI are at a greater risk for unauthorized access, misuse, or loss.

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

To minimize the risk of data loss or suffering a serious interruption of service, school district officials should establish a comprehensive written IT contingency plan. The plan should address the potential for sudden, unplanned disruptions (e.g., ransomware or other malware attack, inadvertent employee action or fire) that could compromise the network and the availability or integrity of the school district's IT system and data, including its applications and PPSI.

Typically, an IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions

needed to maintain or quickly resume operations. The plan should be periodically tested, shared and updated to ensure key officials understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements.

## Officials Did Not Have an IT Contingency Plan

The Board and District officials did not develop and adopt a written IT contingency plan to describe how officials should respond to potential unplanned IT disruptions and disasters affecting the District's IT environment. The District's external auditor commented on the District's lack of an IT contingency plan in the management letter provided to officials each year since 2013-14. Since 2016-17, the external auditor management letters indicated the District contracted with an outside vendor to develop an IT contingency plan; however, the District never developed an IT contingency plan and officials were not able to provide a reasonable explanation for not putting a plan in place back in 2013-14 when the external auditors first reported this deficiency.

Without a comprehensive written IT contingency plan, 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, the District has an increased risk that it could lose important data and suffer a serious interruption in operations.

## What Do We Recommend?

The Board and District officials should:

1. Establish a policy and written procedures that require users to be trained in IT security awareness issues and in proper usage of the IT infrastructure, software and data.

2. Develop and adopt a comprehensive written 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 Director should:

3. Establish comprehensive written procedures for managing network and financial application 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.

5. Ensure users receive periodic IT security awareness training that reflects current risks identified by the IT community.

# Appendix A: Response From District Officials


**MONTAUK UNION FREE SCHOOL DISTRICT**

50 SOUTH DORSET DRIVE
MONTAUK, NEW YORK 11954
TELEPHONE: 631 668-2474
FAX: 631 668-1107
www.montaukschool.org

"The Lighthouse School District"

J. PHILIP PERNA, Superintendent
BRIGID COLLINS, Asst. Principal
P. GRACE LIGHTCAP, District Clerk
FERNANDO OSORIO, District Treasurer


December 6, 2022

Mr. Ira McCrackin
Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, NY 11788-5533

Dear Mr. McCrackin:

This is to acknowledge the audit that was completed this summer at the Montauk UFSD which focused on Information Technology and several weaknesses identified by the auditing team. They were very professional and helpful and we enjoyed working with them and appreciate their help in getting our systems where they need to be.

We agree with most of their findings and we are working to address them. Our IT department is working with our technology consultants to be sure that all of the issues are addressed properly and in a timely fashion.

We understand that some of the student accounts should have been disabled, but the number 97 is inflated. We have student accounts for them to use some of our instructional programs, since they use Chromebooks, they do not need to log on [redacted] computers. In addition, we have student accounts for all students, but the Pre-K students' accounts are for remote instruction if needed.

See Note 1 Page 9

Again, thank you for your assistance.

Sincerely,

J. Philip Perna
Superintendent

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

Note 1

The 97 student accounts not logged into for an extended period of time were identified from our review of the District's enabled network user accounts. During our audit, the IT Director did not provide an explanation as to why the 97 student accounts were inactive and had not been disabled. However, when we inquired about these accounts again after the exit conference, the IT Director informed us that approximately half the 97 user accounts were for students enrolled in the District at the time of our audit test on May 5, 2022, but he did not clarify whether any of the 97 accounts were necessary. We have amended the report to clarify our discussion with the IT Director.

# 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, Treasurer and IT Director to gain an understanding of the IT environment and determine whether:
  - Officials secured and managed user 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 examined network user accounts and security settings on the District's domain controller as of May 5, 2022 using a computerized audit script that identified employee, generic and student user 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 Director to determine whether the user accounts were appropriate and needed.
- We interviewed the Treasurer and IT Director and reviewed software permission reports from the financial application provided by the Treasurer on April 15, 2022 to determine how application user account permissions were managed. We examined the permissions granted to accounts associated with all six business office employees to determine whether the IT Director and Treasurer 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 to develop and adopt an IT contingency plan.

Our audit also examined the adequacy of certain sensitive information technology 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