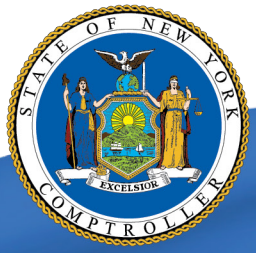
REPORT OF EXAMINATION | 2021M-78

Menands
Union Free School District

Information Technology

NOVEMBER 2021



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

Contents

Report Highlights

Menands Union Free School District

Audit Objective

Determine if the Menands Union Free School District (District) Board of Education (Board) and District officials adequately safeguarded computerized data from unauthorized use, access and loss.

Key Findings

District officials did not adequately safeguard computerized data from unauthorized use, access and loss and although the District paid IT vendors $106,460 for IT services, officials did not have clear contract language that identified the IT vendors' roles and responsibilities. As a result, gaps in IT security practices occurred.

The Board and District officials also did not:

- Monitor internet usage; we found questionable internet use on three of six users' computers examined.
- Provide IT security awareness training to employees.
- Adopt a breach notification policy that is required by New York State Technology Law.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Revise IT vendor contracts to define roles and responsibilities.
- Provide IT security awareness training.
- Develop and adopt a breach notification policy.

District officials agreed with our recommendations and indicated they are taking corrective action.

Background

The District is located in Albany County and serves 325 students in kindergarten through eighth grade. The District pays tuition for an additional 130 Menands students in ninth through twelfth grades to attend one of six area high schools.

The District is governed by an elected five-member Board. The District Superintendent oversees the daily operations along with a District Business Manager/District Treasurer, Deputy Treasurer and District Clerk.

The District contracts with the Capital Region Board of Cooperative Educational Services Northeast Regional Information Center (NERIC) to provide technical support. Additionally, the District has an intermunicipal agreement with South Colonie Central School District to provide an IT technician who serves as the District's network administrator.

Quick Facts	
Network User Accounts	859
Total Paid to IT Vendors During Audit Period	$ 106,460
Employees	107

Audit Period

July 1, 2019 – January 31, 2021

Information Technology

The District relies on its IT assets for a variety of tasks including Internet access; email; and maintaining financial, student and personnel records, which contain personal, private and sensitive information (PPSI). If the IT system is compromised, the results can be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls do not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data may be lost or stolen by inappropriate access or use.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability.

How Should District Officials Safeguard Computerized Data?

A district has a responsibility to safeguard its data to achieve efficient operations and guard against its loss, theft or fraudulent use.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by:

- Monitoring Internet usage,
- Configuring web filtering software to block access to unacceptable websites and help limit access to sites that comply with the acceptable use policy, and
- Providing IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data, and communicates related policies and procedures to all employees and students.

The District's acceptable use policies (AUPs) allowed the use of District IT assets only for educational purposes.

New York State Technology Law requires local governments to adopt a breach notification policy that details actions to be taken to notify affected individuals if their personal information is compromised. The policy should address how officials would notify individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization.

Written agreements with IT vendors define the contractual relationship and responsibilities between the provider and a district, including what services will be provided, when and how they will be provided and at what cost. A written agreement should also describe the internal controls in place to provide reasonable assurance that the local government's information will be protected against unauthorized use, access and loss.

District Officials Did Not Monitor Internet Usage

District employees sign the District employee account agreement (AUP) which limits the use of the information technology system to education and job-related purposes only. However, officials did not monitor employee Internet use. We

reviewed the Internet browsing history for six user accounts belonging to key District officials with access to PPSI and found personal Internet use on three network user accounts. This included online shopping, travel, news and entertainment websites.

The District's agreement with NERIC included web filtering services. The service segregated users into three groups (administration, faculty and staff, and students) and is designed to block users from accessing unauthorized website categories such as gambling or pornography per the District's requirements. The service has the flexibility to block or allow specific sites based on District needs. However, there is no periodic communication between the District and the vendor regarding the District's expectations of the level of service and potential threats (See *Contracts with Third Party IT Vendors Lack Language Regarding Data Security* as follows).

By not monitoring the personal use of District computers, the District increased the risk their computers and network would be exposed to attacks and malicious software. Consequently, PPSI and other computerized data, including financial records and grades, contained on the computers or accessed from users' accounts had a higher risk of breach, loss and/or misuse. District officials stated a high level of access was generally allowed so that faculty could easily access educational material. However, users' levels of access and their web history was not periodically reviewed for reasonableness or adherence to policy.

Further, users have not been provided IT security awareness training because training was not prioritized by the District. To understand current and emerging threats and how to avoid them, users should be regularly and formally trained in IT security awareness.

District officials stated they have never received reports about threats detected or prevented, from any of their outside providers. The absence of regular follow-up and communication with the vendor to review threat activity can erode the District's awareness of threats and hinder their ability to deal with them.

By not monitoring the personal use of District computers, the District increased the risk their computers and network would be exposed to attacks and malicious software.

The Board Did Not Adopt a Breach Notification Policy

Although required by law, the Board did not adopt a breach notification policy. As a result, if PPSI is compromised, the District will not be appropriately prepared to fulfill its legal obligation to notify affected individuals. District officials indicated that the Board did not prioritize development and implementation of such a policy.

Contracts With Third Party IT Vendors Lack Language Regarding Data Security

District officials told us that they rely heavily on the third-party providers for IT support, including monitoring internet activity and safeguarding the District's computerized data. However, the agreements lacked language detailing the performance related to data security.

Without defined language, the roles and responsibilities of each vendor providing services to the District may not be adequately understood by the District. Because contract language does not clearly identify the roles and responsibilities the vendor is to be providing, gaps in IT security practices have occurred. The District has the responsibility to ensure that any contracts with IT vendors adequately address the safety and security of District data. This can be achieved through specific language in the contracts and by a deliberate process of determining, through discussion with the vendor, how security will be achieved.

The District has the responsibility to ensure that any contracts with IT vendors adequately address the safety and security of District data.

What Do We Recommend?

The Board should:

1. Develop and adopt a breach notification policy.
2. Revise IT agreements to include clearly defined roles and responsibilities for each IT vendor and that District data is adequately protected under the terms of the agreements.

District officials should:

3. Review employees' Internet access and use on an ongoing basis to ensure it is in line with the policies.
4. Ensure that employees who use District IT resources receive formal IT security awareness training on a regular basis. This training should include a review of the District's acceptable use policy and best practices for internet use.
5. Establish procedures to review, through communication with IT vendors, compliance with District policies and contractual agreements.

Appendix A: Response From District Officials

Dr. Maureen A. Long
Superintendent of School's
Ext 101

Jennifer Cannavo
Principal
Ext 119

Kathy Cietek
Business Manager
Ext 105

Cheri Vandenberg
Guidance Counselor
Ext 156

Meghan Amatrano
Coordinator of Pupil
Personnel Services
Ext 115

Carin D'Ambro
School Nurse
Ext 109
Fax 518-434-2840

Board of Education

President
Jeff Masline

Vice President
William Nevins

Members
Courtney Jaskula
Andi Delancy
John Diefenderfer

District Clerk
Jeanne Mentiply

Menands Union Free School District

19 Wards Lane, Menands, NY 12204
T (518) 465-4561 F (518)- 434-2840
www.menands.org

October 12, 2021

Gary Gifford Chief Examiner
Office of the State Comptroller
Glens Falls Regional Office
1 Broad Street Plaza
Glens Falls, NY 12801-4396

Unit Name: Menands UFSD
Audit Report Title: Information Technology
Audit Report Number: 2021M-78

Dear Mr. Gifford:

The Menands Union Free School District Administration and Board of Education are in receipt of and have had the opportunity to review the recently completed draft Audit and Confidential IT letter. We thank the Office of the State Comptroller for the professional manner in which the audit was conducted and for the findings; they will serve as a valuable resource in our continued efforts to improve our operations and best serve our students, staff and community, upholding our responsibility to protect and maintain a secure information technology (IT) system.

Following a full review of the audit findings, including discussion during the exit conference conducted with members of your office on September 30, 2021, we are in agreement with the findings of the audit. All key recommendations have been addressed, including those shared in the confidential IT letter. This response to the audit will also serve as our Corrective Action Plan (CAP).

Audit Recommendations:
Develop and adopt a breach notification policy.

Implementation Plan of Action:
The Menands Union Free School District has developed and implemented a comprehensive Breach Notification Policy.

Implementation Date:
June 14, 2021

Person Responsible for Implementation:
Director of IT

Audit Recommendation:

Revise IT agreements to include clearly defined roles and responsibilities for each IT vendor and that district data is adequately protected under the terms of the agreement.

Implementation of Action Plan:

All existing software vendors, both free and paid, are obligated to enter into a Consultant Confidentiality Agreement that is Ed Law 2d compliant. Vendors are required to report to the District any breach notification immediately upon occurrence, must protect data both while at rest and when in motion and must limit access to data to essential employees only. IT contracts with other vendors are currently under review, in collaboration with legal counsel, so that roles and responsibilities are clearly defined and District data is adequately protected.

Implementation Date:

December 10, 2021 and ongoing. With all current contracts to be revised no later than July 1, 2022, and any subsequent contracts meeting this threshold.

Person Responsible for Implementation:

District Superintendent and Business Official in consultation with legal counsel and IT Director.

Audit Recommendation:

Review employee's internet access and use on an ongoing basis to ensure IT is in line with the policies.

Implementation Plan of Action:

The board Policy Committee has reviewed and updated all technology policies related to technology and computer use to ensure they meet the most current recommendations and standards. District IT staff has reviewed and confirmed adequate filter settings. They have also implemented a system of regularly and randomly reviewing user web activity. Such audits will be conducted at a minimum quarterly. Each school year all users (including new hires) will review in writing such policies and relevant training, and will submit an attestation to such.

Implementation Date:

March 25, 2021 and ongoing

Person Responsible for Implementation:

District Superintendent and IT Director

Audit Recommendation:

Ensure that employees who use District IT resources receive formal IT security awareness training on a regular basis. This training should include a review of the Districts Acceptable Use Policy and Best Practice for Internet Use.

Implementation Plan of Action:

The District incorporated formal IT security awareness training as part of monthly faculty meetings and teacher meetings. Additionally as part of the annual Opening Superintendent's Conference Day review of the Districts Acceptable Use Policy will occur with participants required to attest to their participation and understanding.

Implementation Date:

February 23, 2021 and ongoing.

Persons Responsible for Implementation:
District Superintendent and IT Director

Audit Recommendation:
Establish procedures to review, through communication with IT vendors, compliance with District policies and contractual agreements.

Implementation Action Plan:
The district has begun and will continue the process of reviewing all existing contracts with IT vendors to incorporate language that will embed procedures which will allow the district to review and evaluate vendor's compliance with District policies. Subsequent agreements will include such language and procedures.

Implementation Date:
September 30, 2021 and ongoing.

Persons Responsible for Implementation:
District Superintendent and IT Director in consultation with Legal Counsel

On behalf of the Menands Union Free School District, we thank you for taking the time to conduct a fair examination of the Districts Information Technology policies, procedures and practices and the opportunity to improve upon them.

Respectfully Submitted,

Dr. Maureen A. Long
Superintendent of Schools

Mr. James Lovett
Director of IT

Ms. Kathleen Cietek
Business Administrator

Mr. Jeffrrey Masline
President, Board of Education

Mr. William Nevins
Vice President, Board of Education

Mrs. Courtney Jaskula
Board of Education Member

Mr. John Diefenderfer
Board of Education Member

Ms. Andi Delancy
Board of Education Member

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 and evaluated Board policies, procedures, IT contracts and interviewed District officials and third-party IT service providers to obtain an understanding of the internal controls over IT.
- We interviewed District officials to determine whether IT security awareness training was provided to employees.
- We ran a computerized audit script on the District's domain controller. We then analyzed the script results, looking for user accounts and security settings that indicated ineffective IT security controls.
- We compared the District's employee list provided to users identified by the computerized audit script. We evaluated whether any users who were no longer employed by the District still had active accounts in the District's network.
- We used our professional judgement to select six employees assigned to six computers. We selected these individuals because they had access to PPSI and financial data. We ran a computerized audit script on our sample of six computers and the server. We then analyzed results generated by the script, to determine if software updates and patches were updated timely, and unnecessary services had been disabled.
- We ran computerized audit scripts on the six selected computers to determine if PPSI contained on the employees' computers was adequately safeguarded.
- For the six computers selected, we ran computerized audit scripts to review web histories to determine if web sites visited were for District purposes and did not present significant risk to the computerized environment.

Our audit also examined the adequacy of certain 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 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

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

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