REPORT OF EXAMINATION | 2021M-31

Mount Pleasant Central School District

Information Technology User Accounts

JULY 2021

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

Contents

Report Highlights

Mount Pleasant Central School District

Audit Objective

Determine whether Mount Pleasant Central School District (District) officials established adequate controls over user accounts in order to prevent unauthorized use, access and/or loss.

Key Findings

District officials did not establish adequate controls over the District's user accounts to prevent unauthorized use, access and/or loss. Officials did not:

- Monitor compliance with the District's acceptable use policy (AUP).
- Adequately manage network user accounts.

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

Key Recommendations

- Develop and implement procedures to monitor compliance with the AUP.
- Develop written procedures for managing system access that include periodically reviewing user access and disabling network user accounts when access is no longer needed.
- Evaluate all existing network accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.

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

Background

The District is located in the Town of Mount Pleasant, in Westchester County. The District is governed by the Board of Education (Board), which is composed of seven elected members.

The Superintendent is appointed by the Board and is the chief executive officer responsible for day-to-day management, under the Board's direction.

The District contracts with an IT vendor to operate and maintain the District's IT system. The District's IT Director is responsible for overseeing and implementing IT controls as directed by the Board and Superintendent.

Quick Facts	
Network User Accounts[a]	2,567
Employees	385
Students	2,000

a) Includes 416 employee, 1,935 student and 216 generic accounts.

Audit Period

July 1, 2019 – July 8, 2020. We extended our scope forward to October 29, 2020, to complete IT testing.

Information Technology

The District relies on its IT assets for Internet access, email and maintaining financial, personnel and student records, 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, customers, third parties or other individuals or entities. If the IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

District officials should develop procedures for monitoring compliance with the District's AUP.

How Should District Officials Monitor Compliance With the AUP?

A district should have a written AUP that defines the procedures for computer, Internet and email use. The AUP should describe what constitutes appropriate and inappropriate use of IT resources, management's expectations concerning personal use and consequences for violating the AUP.

District officials should develop procedures for monitoring compliance with the District's AUP. Procedures should include routinely monitoring Internet usage and requiring web filtering software to block access to unacceptable websites and limit access to sites that do not comply with the District's AUP.

District Officials Did Not Monitor Compliance With the AUP

The District has an AUP that defines the procedures for computer, Internet, and email use. The policy describes what constitutes appropriate and inappropriate use of IT resources and states that the Internet is to be used exclusively for instructional, research and administrative purposes only. In addition, employees and authorized users are not permitted to access any other email account or system (e.g., Yahoo, Hotmail, AOL) via the District's network or use the District's email programs to conduct job searches or post personal information online (e.g., bulletin boards, blogs, etc.). District officials have not designed and implemented procedures to monitor compliance with the policy. Therefore, monitoring was not performed.

We examined the web browsing history of six computers[1] used by employees whose job duties routinely involved accessing PPSI, to determine whether they were used for personal web browsing purposes. We found evidence of personal use on five of the six employee computers. Such use included the following:

1 Refer to Appendix B for information on our sampling methodology.

- Personal Email
- Social Networking
- Shopping
- Travel
- News
- Music/Entertainment
- Personal Online Banking

District officials were unaware of the questionable Internet use because they did not monitor employee Internet use or implement procedures to monitor for compliance with the District's AUP. The IT Director stated that while the District blocked inappropriate sites such as gambling and pornography for all users, web browser settings did not block staff from websites such as shopping and news because various sites were needed for purchasing and educational purposes.

The District's failure to monitor Internet use increases the risk of improper use by employees and puts the IT system at risk, potentially resulting in the manipulation, destruction or theft of valuable District data or disclosure of PPSI.

How Should District Officials Manage Network User Accounts?

User accounts provide access to networks and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. A district should have written procedures for granting, changing and revoking access rights to the network. In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed. Officials should disable unnecessary accounts as soon as there is no longer a need for them.

District Officials Did Not Adequately Manage Network User Accounts

District officials did not establish procedures to manage network user accounts or maintain a current list of authorized network users and their level of access. As a result, we found unneeded network user accounts that had not been disabled or monitored by the District IT Director.

For example, during our review of the 416 employee network user accounts, we identified 55 network user accounts that did not match the active employee list. District officials stated that 12 of the identified network user accounts were no longer needed and had belonged to 10 employees and two third-party contractors, all of whom are no longer with the District. The remaining 43 network

> …[T]o minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed.

user accounts belonged to independent contractors and employees that had name changes but were still with the District.

Because the District's network had unneeded active user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources.

What Do We Recommend?

District officials should:

1. Develop written procedures to monitor internet usage compliance with the AUP.
2. Develop written procedures for managing system access that include periodically reviewing user access and disabling network user accounts when access is no longer needed.

The IT Director should:

3. Monitor Internet use to ensure employees comply with the AUP.
4. Evaluate all existing network accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.

Appendix A: Response From District Officials

Mount Pleasant Schools

District Office
825 Westlake Drive
Thornwood, NY 10594
Telephone: (914) 769-5500
Email: Kkotes@mtplcsd.org

Dr. Kurtis Kotes
Superintendent of Schools

June 10, 2020

Office of the State Comptroller
Newburgh Regional Office
Lisa A. Reynolds, Chief Examiner
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Dear Ms. Reynolds,

This letter is in response to the Draft Report of Examination 2021M-31: Information Technology User Accounts for the period of July 1, 2019 to October 29, 2020 which was reviewed and discussed at an exit conference held on May 21, 2021. After careful consideration, the Mt. Pleasant Central School District acknowledges the findings and recommendations without dispute. The implementation of corrective measures has already been initiated and a full and complete Corrective Action Plan (CAP) will be prepared and provided to the Comptroller's Office and the State Education Department as required.

On behalf of the District, I would like to express our sincere appreciation to the Comptroller's Office for the time and effort involved in conducting this audit under the uniquely challenging circumstances necessitated by the COVID-19 global health pandemic. The thorough examination by the Comptroller's Office Staff was performed in a professional and courteous manner and their thoughtful feedback will be used to improve District processes and procedures moving forward.

If you have any questions or concerns regarding this response or any other matter relative to this audit, please do not hesitate to contact me.

Sincerely,

Dr. Kurtis Kotes
Superintendent of Schools

CC: Board of Education
Mr. Andrew B. Lennon, Director of Business
Mrs. Vineetha Joy, Director of Technology and Data

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 network user accounts and determine the adequacy of the policies and procedures. We reviewed five acknowledgement forms to verify employees received and read the AUP.
- We inquired with District officials regarding whether they received IT security awareness training and how they are notified of policy changes and updates to the IT policy.
- We ran computerized audit scripts to examine local user account settings and web browsing histories on six employee computers. We used our professional judgment to select six employee computers based on job duties that involve accessing PPSI.
- We ran a computerized audit script to examine the District's domain controller. We then analyzed the report by comparing user accounts to a list of current employees to determine whether any network users were no longer employed by the District.

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.

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
https://www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://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
https://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
https://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
https://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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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