DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-33

Marlboro Central School District

Information Technology

JULY 2021

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

Contents

Report Highlights

Marlboro Central School District

Audit Objective

Determine whether Marlboro Central School District (District) officials established adequate controls over network user accounts and settings.

Key Findings

District officials did not establish adequate controls over network user accounts and settings.

- Officials did not regularly review network user accounts and permissions to determine whether they were appropriate or needed to be disabled.
- 79 percent (71 network user accounts and 14 generic and/or shared user accounts) of the reviewed accounts were unneeded or questionable accounts.
- Officials developed a data security plan in January 2010 that included password security and user account management policies and procedures; however, the Board did not adopt the policy and the practice was not implemented.

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

Key Recommendations

- Develop written procedures for managing system access.
- Restrict the use of shared network user accounts.

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

Background

The District is located in the Town of Marlborough, Ulster County.

The District is governed by an elected seven-member Board of Education (Board). The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's 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 Assistant Superintendent of Personnel and Technology is responsible for monitoring network user accounts and permissions.

Quick Facts	
Student Network Accounts	1,932
Non-Student Network Accounts	386
Students	1,895
Employees	324
2020-21	
Budgeted IT Appropriations	$1.8 million

Audit Period

January 1, 2019 – August 11, 2020

Information Technology

Why Should Officials Manage Network User Accounts?

Network user accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users. These accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view data stored on the network. Therefore, network user accounts should be actively managed to minimize the risk of unauthorized access or misuse.

A district should have written procedures for granting, changing and revoking access rights to the network. To minimize the risk of unauthorized access, officials should regularly review enabled network user accounts to ensure they are still needed. Officials must disable unnecessary or unneeded accounts as soon as there is no longer a need for them, including user accounts of former employees or employees who have transferred to another area.

District Officials Did Not Adequately Manage Network User Accounts

Officials did not adequately manage network user accounts for the District's network. We reviewed all network user accounts and identified 645 accounts that have not been used in more than twelve months. We reviewed 82 of these network user accounts composed of 11 non-student and 71 student accounts. We also reviewed all 26 generic accounts. During our review of the 108 user accounts, we found that 85 accounts (79 percent) were either unneeded or questionable and had not been disabled or adequately managed.

[W]e found unneeded accounts that had not been disabled…

Unneeded Non-Student Accounts – We found that five of the 11 network accounts not used in the last 12 months were for former employees and no longer needed. For example, we found an active network user account for an employee who had retired in 2016. According to District officials, the remaining six non-student user accounts were for active employees and were still needed. User accounts of former employees that have not been disabled or removed could potentially be used by those individuals or others for malicious purposes.

Unneeded Student Accounts – Three of the 71 inactive student accounts were associated with students who were suspended by District administration and were not disabled for the suspension periods. District officials told us that the remaining 68 accounts did not access the network because they were using their personal Google accounts instead. We found that 60 of these accounts were never used to log onto the network. Some of the accounts were created dating back to August 2014. Therefore, the need for these student accounts is questionable. Officials should review these accounts to determine if they are still needed.

Unneeded Generic Accounts – During our review of all enabled user accounts, we identified 26 generic user accounts and found 14 generic accounts that were no longer needed. District officials told us that most of these generic accounts were created for substitutes to log into the virtual monitoring of classes due to COVID-19. However, officials agreed that individual accounts for these substitutes should be created. When allowing multiple user access to a generic account, a lack of proper management can result. Generic accounts increase the risk associated with accountability. It will also affect the transparency and auditing trail that corresponds with the account.

While officials developed a data security plan in January 2010 that included password security and user account management policies and procedures, specifically the removal of dormant user accounts after 12 months, we found that the plan has not been adopted by the Board, nor has this practice been properly implemented or monitored. The IT Director told us the plan was discussed at the Board level, but it was treated as a supporting document to the district technology plan and, therefore, not explicitly approved by the Board. Furthermore, District officials told us they only enable or disable accounts when notified by a department head; however, we found this practice did not always occur.

If unneeded network user accounts are accessed by an attacker, the entry point could be used to inappropriately access and view personal, private and sensitive information (PPSI). Also, having many unneeded user accounts may make it more difficult to manage network access. In addition, because employees shared user accounts, accountability was diminished and activity in the system could not be traced back to a specific user.

What Do We Recommend?

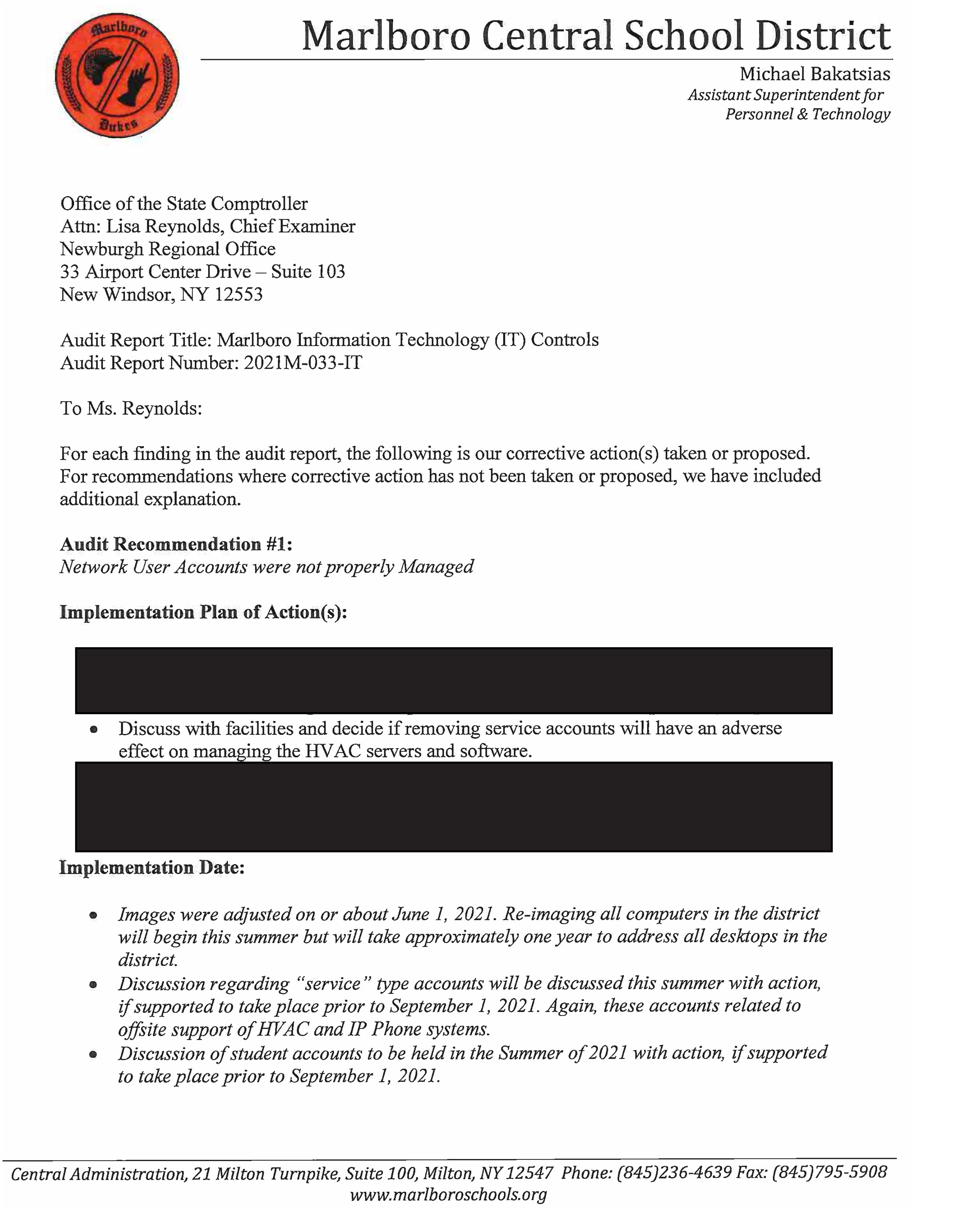
District Officials should:

1. Develop written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed for the network.

2. Restrict the use of shared network user accounts and develop procedures to monitor the use of these accounts.

Appendix A: Response From District Officials

Due to the sensitivity of certain IT information in the response from officials, it was redacted from the report.



Marlboro Central School District

Michael Bakatsias
Assistant Superintendent for
Personnel & Technology

Office of the State Comptroller
Attn: Lisa Reynolds, Chief Examiner
Newburgh Regional Office
33 Airport Center Drive – Suite 103
New Windsor, NY 12553

Audit Report Title: Marlboro Information Technology (IT) Controls
Audit Report Number: 2021M-033-IT

To Ms. Reynolds:

For each finding in the audit report, the following is our corrective action(s) taken or proposed. For recommendations where corrective action has not been taken or proposed, we have included additional explanation.

Audit Recommendation #1:
Network User Accounts were not properly Managed

Implementation Plan of Action(s):

[redacted]

- Discuss with facilities and decide if removing service accounts will have an adverse effect on managing the HVAC servers and software.

[redacted]

Implementation Date:

- *Images were adjusted on or about June 1, 2021. Re-imaging all computers in the district will begin this summer but will take approximately one year to address all desktops in the district.*
- *Discussion regarding "service" type accounts will be discussed this summer with action, if supported to take place prior to September 1, 2021. Again, these accounts related to offsite support of HVAC and IP Phone systems.*
- *Discussion of student accounts to be held in the Summer of 2021 with action, if supported to take place prior to September 1, 2021.*

Implementation Date:
Images were adjusted on or about June 1, 2021. Re-imaging all computers in the district will begin this summer but will take approximately one year to address all desktops in the district.

[redacted]

Depending on discussion of the the remaining items, possible action may be taken on or about September 1, 2021.

Person Responsible for Implementation:
Michael Bakatsias

[redacted]

Implementation Date:

- *IT Staff to discuss and investigate further workstation settings, Summer 2021.*

Person Responsible for Implementation:
Michael Bakatsias

Signed:

____
Name
Assistant Superintendent for Technology & Personnel
6/25/21
Date

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 IT operations, specifically those related to granting, modifying and disabling network user accounts and permissions.
- We examined network user account and security settings using a specialized audit script. We reviewed the network user and administrative accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts. We reviewed automated settings to identify any settings that indicated ineffective IT controls.
- We randomly selected 82 of 645 networked user accounts that had not been accessed since June 30, 2019 to determine if the accounts were needed.
- We examined all 26 generic user accounts to determine if those accounts were properly managed.

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 to 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, Sullivan, Ulster,
Westchester counties

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