DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-48

Millbrook Central School District

Information Technology – User Accounts

AUGUST 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Millbrook Central School District

Audit Objective

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

Key Findings

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

- Periodically review and disable unneeded network user accounts.
  - 46 students were no longer enrolled but had active network user accounts.
  - 13 individuals left employment between 2013 and 2020 but had active network user accounts.
  - Nine generic accounts were last used between 2015 and 2018.
- Develop a breach notification policy, as required by New York State Technology Law.

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

Key Recommendations

- Develop written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed.
- Develop a breach notification policy.

Town officials agreed with our recommendations and indicated they will take corrective action.

Background

The District serves the six Towns of Washington, Union Vale, Clinton, LaGrange, Stanford and Pleasant Valley in Dutchess County.

The District is governed by the Board of Education (Board), which has seven elected members.

The Superintendent is appointed by the Board and is the chief executive officer responsible for, along with other administrative staff, the District's day-to-day management under the Board's direction.

The District's IT Director is responsible for monitoring user accounts.

Quick Facts	
Network User Accounts[a]	1,325
Employees	350
Students	944

[a] These included 208 employee, 1,035 student and 82 generic accounts.

Audit Period

July 1, 2019 – September 4, 2020. We extended our scope forward to November 9, 2020, to complete IT testing.

Information Technology

The District's IT system and data are valuable resources. 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).[1] 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.

How Should Officials Properly Manage Network User Accounts?

User accounts provide access to a district's network and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers to inappropriately access and view PPSI on the network. A district should have written procedures for granting, changing and revoking user permissions 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 must disable unnecessary or unneeded accounts promptly, including user accounts of former employees.

...[D)istrict officials should regularly review enabled network user accounts to ensure they are still needed.

District Officials Did Not Adequately Manage Network User Accounts

District officials did not develop comprehensive written procedures for managing system access and did not adequately manage user accounts for the District's network. According to the IT Director, network user accounts were deactivated immediately upon notification. However, user accounts were not periodically reviewed and there were no procedures in place to ensure IT staff were notified when a student or employee left the District or required a change in permissions. As a result, there is no formal process for notifying the IT Department when an account should be modified or disabled on the District's network.

We reviewed all of the District's 1,325 network user accounts for inactive user accounts.[2] We identified 49 student, 31 employee and 25 generic user accounts that had not been used for more than two years and appeared inactive. After their review of these user accounts, the District disabled 46 of the 49 student and nine of the 25 generic user accounts last used between 2015 and 2018, that were no

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general.

[2] Inactive user accounts are accounts that have not logged into the network during a specified period of time.

longer needed. District officials stated that 15 of the remaining 16 generic network user accounts were created by the computer software and had no direct log-in. Fourteen of the 15 computer-created accounts were needed for email. In addition, 13 of the 31 employee user accounts did not match the current employee list because the employees left the District between 2013 and 2020. After review by the District, these accounts were deemed no longer needed and were disabled. The remaining 18 employee user accounts were identified as Board member or vendor user accounts that were needed. The IT Director indicated that he was not aware the unneeded accounts had not been previously disabled.

Without formal procedures for regularly reviewing enabled user accounts, the District had a greater risk that the unneeded accounts could be compromised or used for malicious purposes. Unneeded network accounts must be disabled promptly to decrease the risk of unauthorized access and potential entry points for attackers.

Why Should District Officials Develop a Breach Notification Policy?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board should establish security policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

New York State Technology Law requires municipalities to adopt a breach notification policy that details actions to be taken to notify affected individuals when there is a system security breach involving personal information.

District Officials Did Not Establish a Breach Notification Policy

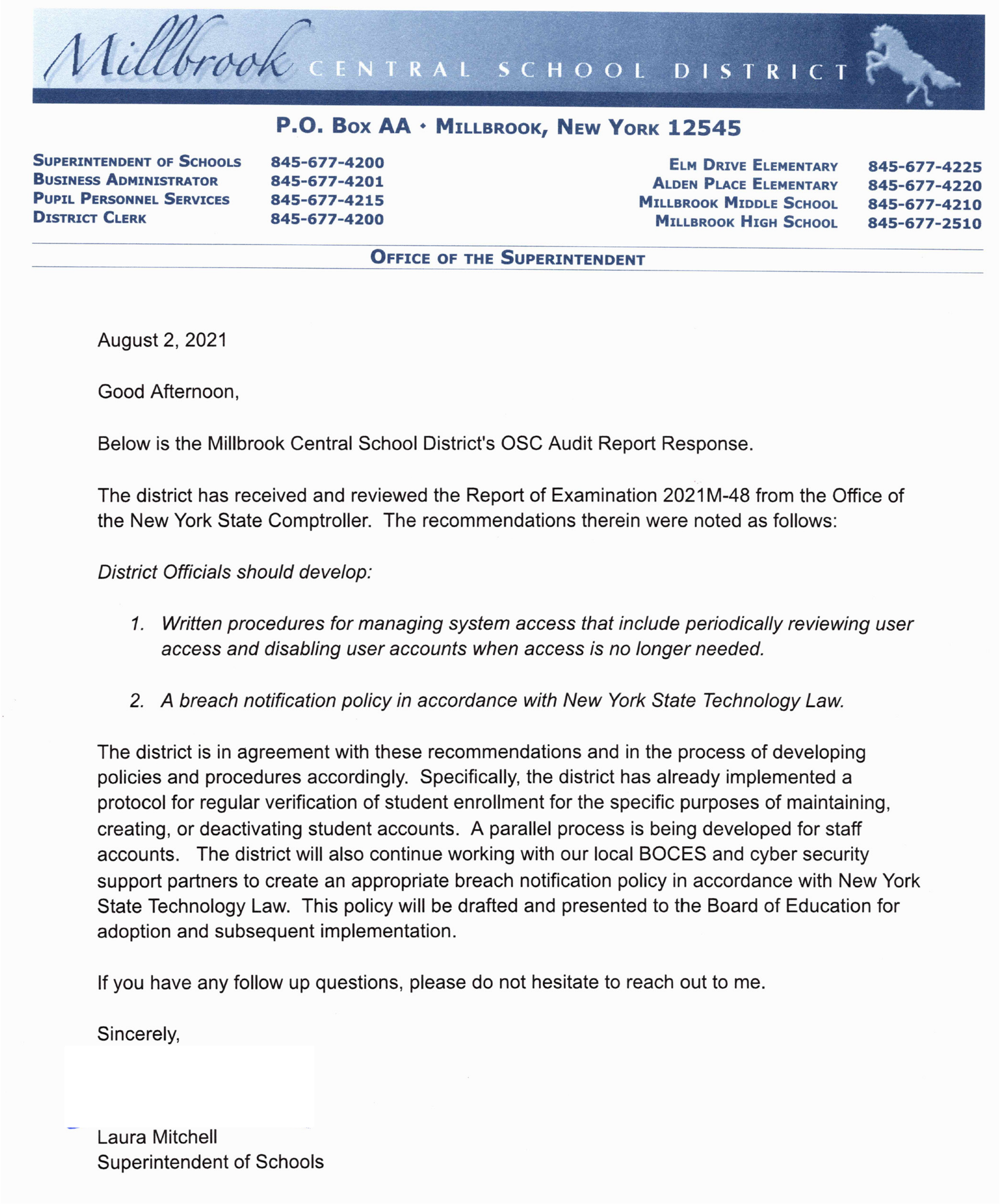
The Board and District officials have not developed and adopted a written breach notification policy because they were unaware of this requirement. As a result, if PPSI is compromised, the District may not be appropriately prepared to fulfill its legal obligation to notify affected individuals.

What Do We Recommend?

District officials should develop:

1. Written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed.
2. A breach notification policy in accordance with New York State Technology Law.

Appendix A: Response From District Officials



Millbrook CENTRAL SCHOOL DISTRICT

P.O. Box AA • Millbrook, New York 12545

Superintendent of Schools	845-677-4200	Elm Drive Elementary	845-677-4225
Business Administrator	845-677-4201	Alden Place Elementary	845-677-4220
Pupil Personnel Services	845-677-4215	Millbrook Middle School	845-677-4210
District Clerk	845-677-4200	Millbrook High School	845-677-2510

Office of the Superintendent

August 2, 2021

Good Afternoon,

Below is the Millbrook Central School District's OSC Audit Report Response.

The district has received and reviewed the Report of Examination 2021M-48 from the Office of the New York State Comptroller. The recommendations therein were noted as follows:

District Officials should develop:

1. *Written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed.*

2. *A breach notification policy in accordance with New York State Technology Law.*

The district is in agreement with these recommendations and in the process of developing policies and procedures accordingly. Specifically, the district has already implemented a protocol for regular verification of student enrollment for the specific purposes of maintaining, creating, or deactivating student accounts. A parallel process is being developed for staff accounts. The district will also continue working with our local BOCES and cyber security support partners to create an appropriate breach notification policy in accordance with New York State Technology Law. This policy will be drafted and presented to the Board of Education for adoption and subsequent implementation.

If you have any follow up questions, please do not hesitate to reach out to me.

Sincerely,

Laura Mitchell
Superintendent of Schools

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 inquired with District officials and employees to obtain an understanding of the District's IT operations, employee IT security awareness training and updates.
- We reviewed District records for any IT-related policies and procedures. Furthermore, we reviewed three acknowledgement forms to verify employees received and read the acceptable use policy (AUP).
- We reviewed service level agreements and interviewed officials to understand the roles and responsibilities of the District's IT staff.
- We ran a computerized audit script on the District's domain controller.[3] 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. We further analyzed generic and student accounts based on last log-on to identify accounts that were no longer needed. We then reviewed the network user accounts and relevant security settings configured on the District's network.
- We ran a computerized audit script on six computers to evaluate whether the Internet use of the six employees was in compliance with the District's AUP. We used our professional judgment to select six employees based on job duties that involve accessing PPSI.
- We used our professional judgment to select a sample of six District computers of employees who had access to PPSI. We ran a computerized audit script on each of the six selected computers to analyze reports generated by the script in order to identify weaknesses in local user account security policies and settings.

Our audit also examined the adequacy of certain 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.

[3] The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

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