New York State Comptroller
THOMAS P. DiNAPOLI

Beacon City School District

Information Technology

2023M-143 | March 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Beacon City School District

Audit Objective

Determine whether Beacon City School District (District) officials ensured network user accounts were adequately managed.

Key Findings

District officials did not ensure network user accounts were adequately managed. Unnecessary enabled network user accounts are additional entry points into a network and, if accessed by attackers, could potentially be compromised or used for malicious purposes. In addition to sensitive information technology (IT) control weaknesses that we communicated confidentially to District officials, we found that officials did not:

- Disable 281 unneeded network user accounts of the 1,280 accounts reviewed, the oldest of which was last used to log into the network in October 2017 as of September 21, 2021. The accounts included:
  - 153 student accounts,
  - 89 nonstudent accounts, and
  - 39 shared and service accounts.
- Develop written procedures for adding, modifying or disabling shared and service accounts.

Key Recommendations

- Disable unneeded network user accounts in a timely manner and periodically review network user accounts for necessity and appropriateness of access.

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

Audit Period

July 1, 2020 – September 21, 2021

Background

The District serves the City of Beacon and portions of the Towns of Fishkill and Wappinger in Dutchess County. The District is governed by an elected nine-member Board of Education (Board) which is responsible for the general management and control of the District's financial and educational affairs.

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

The Director of Technology (IT Director), with assistance from IT staff, is responsible for managing, configuring and securing network user accounts. The Network Specialist is responsible for ensuring the IT systems function correctly.

Quick Facts	
Students	2,579
Employees	870
Enabled Network User Accounts	
Student	2,787
Nonstudent	856
Shared/Service	123
Total	**3,766**
Accounts Reviewed	1,280

Network User Accounts

A school district's (district's) IT system and data are valuable resources. A district relies on its network and IT assets for maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI)[1] and are accessed through network user accounts, email and Internet access. If the network or IT assets are compromised or disrupted, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and/or rebuild. While effective controls, such as adequately managed, configured and secured network user accounts, will not guarantee the network or IT assets' safety, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

How Should District Officials Manage Network User Accounts?

Because network user accounts provide access to network resources, district officials should actively manage them to minimize the risk of unauthorized access and misuse. Therefore, districts should have written procedures for granting, changing and disabling network user accounts, along with evaluating and adjusting these procedures, as needed, to ensure all processes to add, modify and disable accounts are working as intended.

District officials should periodically review and disable unnecessary accounts as soon as they are no longer needed. In addition, to minimize the risk of unauthorized access, officials should regularly review enabled network user accounts to ensure they are still needed.

Shared and service network user accounts should be limited in use as they are not linked to one individual and therefore may have reduced accountability. Shared user accounts are accounts with a username and password that are shared among two or more users, and are often used to, for example, provide access to guests or other temporary or intermittent users (e.g., substitute teachers and third-party vendors). Service accounts are accounts created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems). District officials should limit the use of shared and service accounts, routinely evaluate the need for the accounts and disable those that are not related to a current district or system need.

Officials Did Not Adequately Manage Network User Accounts

The former IT Director, who left the District in May 2022, and his staff were responsible for ensuring that the District's network user accounts were managed

1 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 individual or entities.

in a timely and adequate manner. We determined that District officials had a process for adding, disabling or modifying employee, student and contractor user accounts. A clerk in the Human Resources department maintained a spreadsheet of when employees started with and separated from the District, and the spreadsheet was used to inform the IT department of new employees and separations. However, District officials did not develop written procedures to convey management's expectations for adding, disabling or modifying shared and service accounts. We inquired with various IT department staff and were told that the former IT Director did not develop procedures for shared and service accounts.

We reviewed all 1,157 enabled network user accounts (assigned to students, employees and contractors) that had not been used in at least six months to determine whether they were still needed. We determined that 242 of the 1,157 network user accounts (21 percent) were no longer needed and should have been disabled, including 153 student accounts and 89 nonstudent accounts. Examples of employees who were assigned nonstudent accounts that should have been disabled included nurses, transportation employees and former business office staff. These users all left the District between October 2017 and September 2021. We also reviewed all 123 enabled shared and service accounts and determined that 39 accounts (32 percent) were no longer needed and should have been disabled.

The Network Specialist told us that the process for disabling employee accounts was not working because the spreadsheet was not always updated when an employee left the District and network user accounts were not periodically reviewed to determine whether they were still needed. In addition, the Network Specialist stated that the shared and service accounts were not disabled because these accounts were created for specific purposes, such as for a server or specific software. The Network Specialist further stated that, when the server or software were no longer needed, the accounts would have very limited rights. However, the accounts would still be potential entry points for an attacker to gain access to the District's network. In addition, these accounts could have administrative network access that would not be limited once the server or software were discontinued.

Unnecessary enabled network user accounts are additional entry points into a network and, if accessed by attackers, could potentially be compromised or used for malicious purposes. In addition, the lack of effective controls over the network user accounts significantly increases the risk of unauthorized use, access and loss.

What Do We Recommend?

The IT Director and/or Network Specialist should:

1. Develop written procedures for adding, modifying and disabling shared and service accounts, and evaluate and adjust these procedures, as needed, to ensure all processes are working as intended.

2. Disable unneeded network user accounts in a timely manner and periodically review network user accounts for necessity and appropriateness of access.

Appendix A: Response From District Officials

BEACON CITY SCHOOL DISTRICT
ADMINISTRATIVE OFFICES
10 Education Drive
Beacon, New York 12508
845-838-6900 phone
845-838-6905 fax

Ms. Ann Marie Quartironi
Deputy Superintendent

Dr. Sagrario Rudecindo-O'Neill
Assistant Superintendent of Curriculum & Student Support

Dr. Heather Chadwell Dennis
Assistant Superintendent of PPS

Dr. Matthew Landahl
Superintendent

February 21, 2024

Office of the State Comptroller
33 Airport Center Drive
Suite 103
New Windsor, NY 12553-4725
Attn: Dara Disko-McCagg

Dear Ms. Disko-McCagg:

In order to ensure the network user accounts in the Beacon City School District are adequately managed, we will disable all unneeded network user accounts in a timely manner. We will also periodically review network user accounts for necessity and appropriateness of access and make any necessary modifications.

The district will develop written procedures for adding, modifying and disabling share and service accounts and evaluate and adjust procedures to ensure all processes are working as intended.

We will begin the corrective action plan process and address how we will implement the procedures mentioned above.

Sincerely,

Dr. Matthew Landahl
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. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of how the District's network user accounts were managed, and determine what procedures existed for adding, disabling or modifying employee, student and contractor user accounts.
- We ran a computerized audit script on the District's domain controller on September 21, 2021. This script produced a list of all enabled network user accounts that had not been used to log into the network within the last six months. We reviewed these accounts with the former IT Director to determine whether they were needed. We compared the accounts the former IT Director identified as needed to a list of current employees and students to determine whether these employees and students were still employed by or enrolled in the District. We discussed all remaining accounts not verified as current employees or students with the former IT Director. We reviewed all shared and service accounts with the former IT Director and Network Specialist to determine whether these accounts were necessary.

Our audit also examined the adequacy of certain sensitive network user account 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 GAGAS (generally accepted government auditing standards). 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.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/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.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.ny.gov/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

https://www.osc.ny.gov/local-government

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief of Municipal Audits

33 Airport Center Drive, Suite 102 • New Windsor, New York 12553-4725

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

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties