New York State Comptroller
THOMAS P. DiNAPOLI

Southern Westchester Board of Cooperative Educational Services

Information Technology

2024M-38 | August 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Southern Westchester Board of Cooperative Educational Services

Audit Objective

Determine whether Southern Westchester Board of Cooperative Educational Services (BOCES) officials secured nonstudent network user accounts, maintained adequate inventory records for information technology (IT) equipment and developed an IT contingency plan.

Key Findings

BOCES officials did not adequately secure nonstudent network user accounts, maintain complete and accurate IT inventory records and develop an IT contingency plan. As a result, BOCES officials cannot ensure that IT systems, which contain personal, private and sensitive information (PPSI), along with physical IT assets, are properly safeguarded from inappropriate use and access.

In addition to sensitive IT control weaknesses that we communicated confidentially to BOCES officials, we determined that:

- 101 enabled nonstudent network accounts were no longer needed and, if accessed by attackers, could be used to inappropriately access and view personal, private and sensitive information or disable the network.
- 16 IT assets could not be traced to or from BOCES' inventory system and 40 IT assets were not properly recorded in the system.

Key Recommendations

- Develop written procedures for managing network user accounts.
- Maintain complete, accurate and up-to-date inventory records.
- Develop and adopt a comprehensive written IT contingency plan.

BOCES officials agreed with our findings and indicated they have initiated corrective action.

Audit Period

July 1, 2022– September 27, 2023

Background

BOCES delivers educational and administrative services to 32 component school districts and is governed by a seven-member Board that is responsible for the general management and oversight of BOCES' financial and educational affairs.

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

BOCES has a service level agreement with the Lower Hudson Regional Information Center (LHRIC) for providing project and services management, as well as system and technical support services. The Director of Technology (IT Director) is responsible for IT functions, including managing network user accounts and maintaining IT inventory records.

Quick Facts	
Total Nonstudent Network User Accounts	1,333
Total Number of IT Asset Inventoried	1,572
IT Assets Tested	40

Information Technology

How Should Officials Secure Nonstudent Network User Accounts?

Network user accounts provide access to network resources and data needed by employees to complete job duties and other work-related responsibilities. BOCES officials should secure all network user accounts, including nonstudent network user accounts (e.g., staff accounts, shared and service accounts and third-party vendor accounts). To help secure these accounts, BOCES officials should actively manage network user accounts, including their creation, use and dormancy, to ensure they are appropriate and authorized. User accounts that are no longer needed should be disabled immediately.

BOCES officials should identify the cybersecurity risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the Board, Superintendent and IT department.

Officials should establish written procedures to help guide network and system administrators in properly granting, modifying and disabling user account access to BOCES networks. These procedures should require BOCES officials to periodically review enabled user accounts to ensure they are appropriate and authorized. IT officials should determine the length of inactivity that indicates a dormant account. Disabling accounts in a timely manner is important because a dormant account could indicate a user account is no longer associated with an active employee and is unnecessary for the performance of duties. Leaving such an account active could allow for inappropriate access by an unauthorized individual.

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. BOCES officials may have difficulty managing the accounts and linking any suspicious activity to a specific user. A shared user account has a username and password that is shared among two or more people and can be used to, for example, provide access to guests or other temporary or intermittent users. A service account is created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems). BOCES officials should routinely evaluate the need for the accounts and disable those that are not related to a current BOCES or system need.

Officials Did Not Adequately Secure Nonstudent Network User Accounts

BOCES officials did not properly secure nonstudent network user accounts. The IT Director did not develop written procedures for granting, changing, disabling and reviewing network user account access to the network. The IT Director told us that BOCES has informal procedures for managing network user

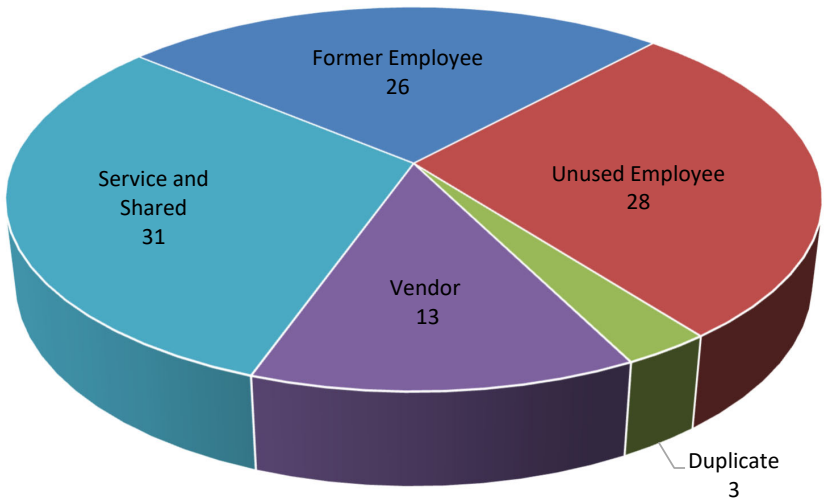
accounts. Specifically, employee network user accounts are created and disabled automatically through BOCES' financial application based upon the hire date and/or separation date entered into the application by personnel from the human resources (HR) department. Vendor network accounts are manually created by the IT Director based on the contract with the vendor, and the account is disabled manually by the IT Director when the BOCES supervisor responsible for the contract informs the IT Director that the network account is no longer needed. Service and shared accounts are managed by the department or individuals they are created for, and the respective department and individuals would notify the IT Director when a service or shared network account is no longer needed.

In addition, the IT Director told us that he reviews the enabled network user accounts once a year and removes any unneeded accounts. However, BOCES' informal network user account management procedures, including the IT Director's annual review, were inadequate and resulted in unneeded accounts that were not disabled as soon as they were no longer needed. For example, one network user account remained active for eight years after the user left BOCES employment, and was disabled after we shared this deficiency.

We reviewed all 1,333 enabled nonstudent network user accounts, including 956 individual network user accounts and 377 service and shared accounts, and determined that 70 individual network user accounts (including former, unused, and duplicate employee accounts and vendor accounts) and 31 service and shared accounts were unneeded (Figure 1) and should have been disabled by the IT Director.

FIGURE 1

Unneeded Nonstudent Network User Accounts



Unnecessary Individual Network User Accounts – We determined that 70 individual user accounts were not needed and should have been disabled, as follows:

- 26 user accounts were assigned to former BOCES employees, including 19 accounts that had an end date in the financial system ranging from September 2015 to September 2023. The IT Director told us that the end date of former employee accounts may have been overridden and frozen for a period of time to have access to the individual's data and email. However, he agreed that these 26 accounts were no longer necessary and subsequently disabled the accounts or requested that they be inactivated after our inquiry.
- Three duplicate accounts were assigned to two current employees and one former employee. The IT Director told us that for a period of time, there was a problem with the system creating duplicate network user accounts. For example, when an employee went from a contracted status to a fulltime employee, the financial application created a new username and network account. He stated that this error was resolved for about a year and agreed that the three user accounts should be disabled.
- 13 user accounts were associated with vendors that did not have active contracts with BOCES. The IT Director indicated that these accounts were disabled after our inquiry.
- Five user accounts were assigned to salaried employees that have never been used, with creation dates ranging from July 2010 to December 2021. The IT Director stated that three accounts were for substitutes that may not have been contacted to work or had a one-on-one assignment that did not require them to log in to the account. For the other two user accounts, he told us the nature of the employees' assignments did not always require a login to the system, but they had network accounts for HR announcements regarding trainings and other BOCES communications. However, the accounts should have been disabled after a period of inactivity and re-enabled in the event the user needed to log in to the system.
- 23 user accounts were assigned to non-salaried (contracted) employees that have not been used in over six months, including nine that have never been used. The IT Director told us that there were no written procedures for disabling contracted employee accounts, but it was the responsibility of the respective BOCES supervisor to inform him when an account is no longer necessary and should be disabled. We followed up with the Assistant Superintendent for Business and Administrative Services (Assistant Superintendent) to determine when the contracted employees were last

compensated by BOCES and if the network user accounts were still needed. We determined that 12 contracted employees were last paid between 2018 and 2021, three in 2022, six in 2023, and two were never paid by BOCES. When network user accounts are not disabled as soon as they are no longer needed, there is an increased risk that, if the network account is compromised, student data and other BOCES applications and systems accessible through that compromised account, such as email, could be inappropriately accessed and possibly used for malicious activity.

Unneeded Shared and Service Network User Accounts – We reviewed all 377 shared and service network user accounts and determined that 31 were unneeded and should have been disabled, as follows:

- 18 service and shared accounts that the IT Director indicated were unnecessary and should have been disabled.
- Five service accounts that BOCES officials identified as to be deleted, but the IT Director told us that the procedure to automatically disable the user accounts was not followed correctly and the accounts remained active. The user accounts were disabled after our inquiry.
- Eight shared accounts were used for financial application training purposes that have not been used since 2020. The IT Director indicated that these accounts are needed even though they have not been accessed since 2020. However, if the accounts are needed, they should be disabled after a period of inactivity and enabled when they are needed again.

Because there were no written procedures in place for IT officials to review network user accounts and informal procedures for disabling shared, service and vendor accounts were not adequate, unneeded accounts were not identified by IT officials until our audit. Shared and service accounts should be limited, as officials may have difficulty managing shared accounts and linking any suspicious activity to a specific user. When network user accounts are not used or monitored, compromised accounts may not be detected in a timely manner.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could severely disrupt BOCES operations or be used to inappropriately access the BOCES network to view and/or remove personal information; make unauthorized changes to BOCES records; or deny legitimate access to the BOCES network and records.

How Should Officials Maintain Adequate IT Inventory Records?

The Board-adopted Personal Property Accountability policy (Policy) requires all IT assets over $500 and a useful life of one year or more to be inventoried. The Policy also requires the Assistant Superintendent or designee to develop, in writing, the basic rules and regulations to be followed in maintaining BOCES' personal property records, which includes IT asset inventories. In addition, the Policy requires that inventory records contain sufficient information to identify each item classified as personal property, including:

- A sufficient description of the personal property,
- The class of personal property (machinery, equipment, etc.),
- The year of acquisition of the personal property,
- The historical cost (the cost at acquisition) of the personal property or the estimated value if the cost is unknown or the item is a gift, and
- The source of financing or acquisition (general fund, federal fund, gift, etc.).

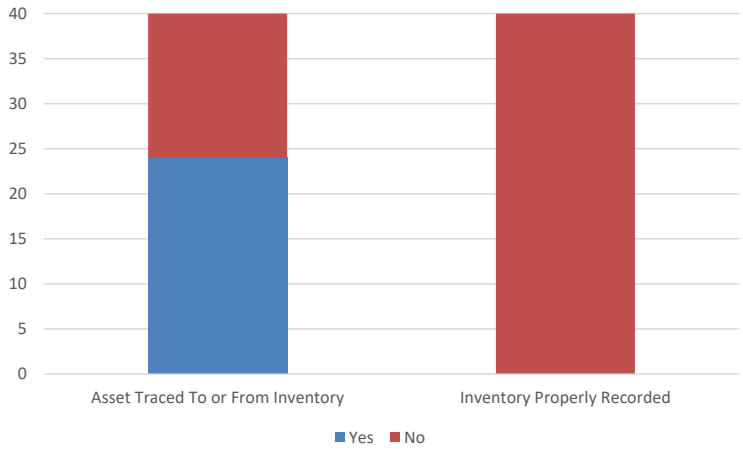
Furthermore, BOCES officials should maintain detailed, up-to-date inventory records for all IT equipment. The information maintained for each piece of IT equipment should include a description of the item, including the make, model and serial number; the name of the employee or authorized individual to whom the equipment is assigned; the physical location of the asset; and the relevant purchase or lease information, including the acquisition date.

Officials Did Not Maintain Adequate IT Inventory Records

Officials did not maintain adequate inventory records. Although the Board-adopted Policy provided direction for officials to track and inventory IT assets and lists the attributes required to be included in tracking inventory records, the Policy did not require that inventory records contain the physical location of the asset or the name of the employee or authorized individual assigned to the asset. In addition, BOCES officials did not adopt written procedures for maintaining inventory records. As a result, we could not trace 16 of 40 IT inventory assets tested (40 percent) to and from the inventory records and the location of the asset. We also determined that all 40 IT assets were not properly recorded, as the inventory listings were missing required attributes (Figure 2).

FIGURE 2

IT Asset Inventory



We selected 20 IT assets from BOCES' inventory listings to trace to the physical location of the asset to determine whether they were properly recorded. We were not able to trace seven IT assets to a physical location, including four iPads and three laptops. The IT Director told us the four iPads and one laptop were lost, and the other two laptops were recycled in February and July in 2023. However, the inventory records were not updated to contain up-to-date information on the status or location of the seven IT assets. In addition, although we were able to trace two laptops belonging to the Superintendent and Director of Business, they both had secondary laptops in their possession that we were not able to trace to the inventory listings. In addition, we conducted an inventory walkthrough and selected 20 IT assets to trace to the inventory listings. We determined that nine IT assets were not recorded in the inventory listings.

Furthermore, for the 31 out of the 40 IT assets selected that were on the inventory listings, the following information was not included:

- 24 assets did not have the purchase price,
- 13 assets did not have the acquisition date,
- 10 assets did not have a location, and
- Eight assets did not have an individual assigned to the asset.

Without complete up-to-date inventory records, officials cannot be assured that IT assets are adequately accounted for and would be detected if lost, stolen or misused. Furthermore, complete, accurate and up-to-date inventory records help

officials ensure that IT assets are properly insured, tracked through their life cycle and replaced as necessary.

Why Should the Board and Officials Develop and Adopt an IT Contingency Plan?

To help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster, the Board and BOCES officials should develop and adopt a comprehensive written IT contingency plan. An IT contingency plan is a recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations after an unexpected IT incident, such as power outages, software or hardware failures caused by a virus or other type of malicious software (e.g., ransomware), human error, equipment destruction or a natural disaster (e.g., flood, fire).

An IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to recover data and quickly resume operations in the event of an unplanned disruption. Additionally, IT contingency plans should include data backup procedures, such as ensuring backups are stored off-site and off-network, and requiring IT staff to periodically test backups to ensure they will function as expected. BOCES officials should periodically test and update the plan, as needed, to help ensure officials understand their roles and responsibilities during and after a disruptive event. Testing and updating IT contingency plans are particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks. These plans should be distributed to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements such as statutory changes.

The Board and Officials Did Not Develop and Adopt an IT Contingency Plan

The Board and BOCES officials did not develop and adopt an IT contingency plan to document and inform staff how they should respond to unplanned disruptions and disasters affecting BOCES' IT environment and procedures for backing up data. The IT Director told us that BOCES relied on LHRIC for their disaster recovery plan, and that while BOCES has informal procedures in place for data recovery, a formal written plan was never developed.

As a result of our audit, the Board developed a draft IT contingency plan to be approved and adopted after we brought the issue to their attention. However, the plan and written procedures were not developed during the audit period. Without a fully developed and implemented IT contingency plan, BOCES officials cannot guarantee that in the event of a disruption or disaster, such as a ransomware

attack, employees would be able to help resume, restore, repair and/or rebuild critical IT systems, applications or data in a timely manner. Depending on the severity of the incident, officials may need to expend significant time and financial resources to resume BOCES operations. Furthermore, responsible parties may not be aware of their roles, complicating BOCES' ability to recover from an incident. As a result, important financial and other data could be lost, or BOCES could suffer a disruption to operations that depend on its computerized environment.

What Do We Recommend?

The Board should:

1. Adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.
2. Update the Policy to include adequate attributes for tracking inventory.

The IT Director should:

3. Maintain complete, accurate and up-to-date inventory records.
4. Develop written procedures on adding, removing, modifying and reviewing user access rights.
5. Disable network user accounts of employees as soon as they leave BOCES employment and disable other unneeded network user accounts in a timely manner.
6. Develop written procedures that include the rules and regulations for maintaining BOCES personal property records, and distribute the procedures to all responsible parties.

Appendix A: Response From BOCES Officials

BOCES Southern Westchester
THE BOARD OF COOPERATIVE EDUCATIONAL SERVICES

17 Berkley Drive, Rye Brook, New York 10573
(914) 937-3820 • fax (914) 937-7850

Friday, July 26, 2024

Dara Disko-McCagg
Chief of Municipal Audits, Newburgh Regional Office
Local Government and School Accountability
33 Airport Center Drive, Suite 102
New Windsor, NY 12553

Ms. Disko-McCagg,

Please consider this correspondence to be the formal response to the preliminary draft findings and recommendations presented to us and reviewed on July 22, 2024.

Southern Westchester BOCES agrees with the findings and has either completed or is in the process of completing all recommended corrective actions.

Thank you for your time and feedback.

Sincerely,

John V. Filibert
Board President

Harold A. Coles, Psy. D.
District Superintendent

COMPONENT DISTRICTS: Ardsley, Blind Brook, Bronxville, Byram Hills, Dobbs Ferry, Eastchester, Edgemont, Elmsford, Greenburgh Abbott, Greenburgh Central Seven, Greenburgh Eleven, Greenburgh Graham, Greenburgh North Castle, Harrison, Hastings-on-Hudson, Hawthorne Cedar Knolls, Irvington, Mount Pleasant Blythedale, Mount Pleasant Central, Mount Pleasant Cottage, Mount Vernon, New Rochelle, Pelham, Pleasantville, Pocantico Hills, Port Chester, Rye City, Rye Neck, Scarsdale, The Tarrytowns, Tuckahoe, Valhalla, White Plains

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 BOCES IT policies and procedures and interviewed the Assistant Superintendent and IT Director to gain an understanding of the IT environment and internal controls surrounding IT assets.
- We ran computerized scripts on September 27, 2023 to identify all enabled network user accounts. We excluded all network user accounts associated with students from our audit testing. We compared the remaining 1,333 enabled nonstudent network user accounts to the active employee list to identify potentially unneeded accounts. We followed up with the IT Director to determine whether the accounts were needed or should have been disabled.
- We used our professional judgment to select a sample of 20 IT assets to trace from the inventory listings to the physical location of the asset. We performed a walkthrough of BOCES facilities and used our professional judgment to select 20 IT assets to determine whether the assets were accurately recorded in the inventory listings. We observed and recorded their tag number, make, model and serial number, location, and the individual assigned to the asset (if applicable).

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 BOCES 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. We encourage the Board to make the CAP available on BOCES' 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