New York State Comptroller
THOMAS P. DiNAPOLI

Ulster Board of Cooperative Educational Services

Network User Accounts

2023M-42 | August 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Ulster Board of Cooperative Educational Services

Audit Objective

Determine whether Ulster Board of Cooperative Educational Services (BOCES) officials adequately managed and monitored network user accounts in order to help prevent unauthorized use, access and loss.

Key Findings

BOCES officials did not adequately manage and monitor network user accounts to help prevent unauthorized use, access, or loss. As a result, BOCES had an increased risk of inappropriate access by users with malicious intent. In addition to sensitive information technology (IT) control weaknesses that were communicated confidentially to BOCES officials, we found that officials did not:

- Disable 17 unneeded network user accounts, including seven former employee accounts and 10 accounts not used by active employees, that had last log on dates ranging from November 2016 to December 2021.
- Review and disable 76 potentially unneeded user accounts, including 34 shared accounts, 31 service accounts, eight vendor accounts and three service accounts.

Key Recommendations

- Develop written procedures for granting, removing and modifying network user account access and ensure these procedures are being followed.
- Periodically review existing network user accounts and disable user accounts when access is no longer needed.

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

Background

BOCES is composed of eight component school districts and is governed by an 11-member BOCES Board (Board) elected by the boards of the component districts. The Board is responsible for the general management and oversight of BOCES' financial and educational affairs.

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

BOCES operates the Mid-Hudson Regional Information Center (MHRIC) that serves 47 school districts in Orange, Dutchess, Sullivan and Ulster counties. The Operations and Programming Manager (Manager), along with the Network Security Specialist (Specialist), are responsible for managing and monitoring BOCES network user accounts. The Director of MHRIC is responsible for overseeing the IT staff.

Quick Facts

Network User Accounts	
Needed	151
Unneeded:	
Former/Unused Employee	17
Service/Shared	68
Vendor	8
Total	**244**

Audit Period

July 1, 2021 – July 21, 2022. We extended our scope through September 21, 2022 to complete our IT Testing.

Network User Accounts

Network user accounts provide access to network resources and should be actively managed and monitored to help minimize the risk of unauthorized use, access and loss. If network user accounts are not properly managed and monitored, unnecessary user accounts may not be detected and disabled timely. Unnecessary accounts are additional entry points for attackers to potentially access and then attempt to view personal, private and sensitive information (PPSI)[1] on the network.

How Should Officials Manage and Monitor Network User Accounts?

To prevent unauthorized use, access and loss, BOCES officials should manage and monitor network user accounts, and disable unnecessary accounts when they are no longer needed, maintain a list of authorized user accounts and regularly review enabled network user accounts to ensure they are needed.

BOCES officials should limit the use of service and shared accounts, routinely evaluate the need for them and disable those that are not related to a current BOCES, or system need. A service account is created for the sole purpose of running a particular network or system service or application (e.g., backups). Shared user accounts have a username and password that are shared among two or more users and are used, for example, to provide access to guests and other temporary or intermittent users. Because service and shared accounts are not assigned to an individual user, accountability may be reduced, and officials may have difficulty managing them and linking suspicious activity to a specific user.

BOCES officials should establish written procedures for actively managing network user accounts – including their creation, use and dormancy – and regularly monitor procedures to ensure accounts are appropriate and authorized.

Officials Did Not Adequately Manage and Monitor Network User Accounts

BOCES officials established informal procedures to manage network user accounts when an employee is hired or terminated. Specifically, the Human Resources (HR) department should send an onboarding/offboarding checklist to BOCES officials and appropriate personnel, including the IT department, which IT staff use to grant, disable or modify access to network user accounts. The Manager stated that changes should be made by IT staff within 24 hours of receiving the checklist from the HR department.

---

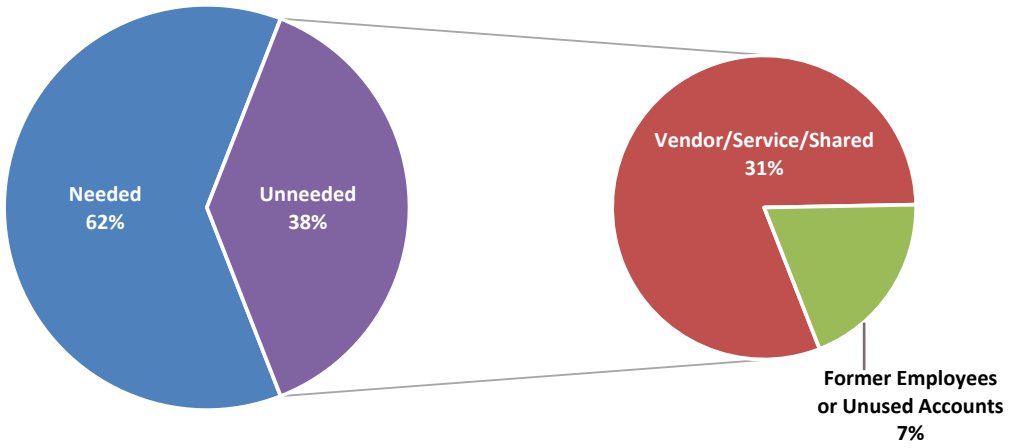
1 PPSI is any information where unauthorized access, disclosure, modification, destruction or use – or disruption of access of use – could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

BOCES officials did not ensure that network user accounts were adequately managed and monitored. The Manager and Specialist were responsible for ensuring that BOCES network user accounts were managed in a timely and satisfactory manner. Although BOCES officials had informal procedures in place for managing and monitoring employee network user accounts, they did not have written procedures for actively managing all network user accounts, including service and shared user accounts.

We examined all 244 enabled network user accounts to determine whether any were unneeded. We found that 93 network user accounts (38 percent), including 76 vendor/service/shared accounts (31 percent) and 17 former and unused employee user accounts (7 percent) were unneeded (Figure 1).

FIGURE 1

Network User Accounts



We compared the BOCES employee master list to the enabled network user accounts and inquired about 36 network user accounts that were not listed as employees. We determined that 18 of the 36 accounts were unneeded (seven former employee accounts, eight vendor accounts and three service accounts) and have not been used in over six months. The oldest unneeded user account was a vendor account that was last logged into in July 2015.

We selected three of the former employee accounts to determine whether the HR department completed the informal procedure of sending the offboarding checklist to IT staff to disable their network user account access. We confirmed that the HR department sent emails to IT staff notifying them of the change for two of the former network user accounts selected. The Director of HR said that the third user account belonged to a former consultant and not an employee, so the form was

not sent to IT staff to disable the account. Although IT staff received an email from the HR department with an offboarding checklist for two of the three accounts reviewed, the network user accounts were not disabled.

Further, we reviewed all 107 enabled employee network user accounts and found that 15 enabled employee accounts have not been used in over six months. We inquired with the Specialist on the reasons why the 15 accounts had not been used and determined that 10 of the 15 network user accounts were no longer needed and should have been disabled, as the employees transferred to a different service area, retired or did not require the network user account based on their job duties. The last login date for the 10 employee accounts ranged from November 2016 to December 2021. The Manager and Specialist told us that former employee accounts were not removed or disabled because IT staff did not receive the offboarding checklist from the HR department.

We reviewed the remaining 101 network user accounts and although the Specialist told us that all 101 of these network user accounts are necessary, 34 shared and 31 service accounts have not been used in over six months and may not be needed. The Manager and Specialist said that BOCES had no written procedures in place to monitor these shared and service accounts but going forward, upon our inquiry, they will be disabled after 90 days of inactivity.

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 timely.

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. When an organization has many network user accounts that must be managed and monitored, unneeded network user accounts increase the risk of inappropriate access by users with malicious intent.

What Do We Recommend?

The Board should:

1. Develop written procedures for granting, disabling and modifying network user account access and implement a process for monitoring compliance with the procedures once they are established to ensure they are being followed.

The Manager and Specialist should:

2. Disable network user accounts of employees as soon as they leave BOCES employment and disable other unneeded network user accounts in a timely manner.

3. Perform a periodic review of existing network user accounts, including shared, service and other non-employee accounts, to limit enabled user accounts to those deemed necessary for BOCES operations.

Appendix A: Response From BOCES Officials

SHARED VISION
SHARED COMMITMENT
SHARED SUCCESS
ULSTER BOCES
BOARD OF COOPERATIVE EDUCATIONAL SERVICES

OFFICE OF THE DISTRICT SUPERINTENDENT
Jonah M. Schenker
District Superintendent

175 Route 32 North • New Paltz, NY 12561
Telephone: 845-255-3040 • Facsimile: 845-255-7942
Email: jschenker@ulsterboces.org • www.ulsterboces.org

July 31, 2023

Office of the State Comptroller
Newburgh Regional Office
ATTN: Dara Disko-McCagg
33 Airport Center Drive, Suite 102
New Windsor, NY 12553

RE: ULSTER BOCES AUDIT – NETWORK USER ACCOUNTS

Dear Ms. Disko-McCagg:

Ulster BOCES is in receipt of the Office of the State Comptroller's draft report relating to the audit of Network User Accounts during the period of July 1, 2021 – September 21, 2022.

Ulster BOCES appreciates the work and professionalism of your audit team throughout the review of the network user accounts. Ulster BOCES strives to continuously improve our processes and procedures. We have a dedicated team working hard to maintain network security.

The draft audit report has been reviewed by the Ulster BOCES Board of Education and our Senior Administrative team. Ulster BOCES accepts the conclusions provided by the Office of the State Comptroller. The development of a corrective action plan is underway and will be submitted for your review within 90 days of the release of the audit.

Thank you for your review of our network user accounts and subsequent recommendations for improvement.

Sincerely,

Jonah M. Schenker, Ed. D.
District Superintendent

JS/rb

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 BOCES IT policies and procedures and interviewed the District Superintendent, School Business Director, Manager and Specialist to gain an understanding of the IT environment, internal controls and training. We met with the Manager and Specialist to determine whether any enabled network accounts were no longer needed and if so, to gain an understanding of why the accounts remained on the network.
- We ran a computerized audit script on the BOCES domain controller on September 21, 2022. We analyzed the reports generated by the script to identify weaknesses in network user account management. We compared the list of enabled network user accounts generated by the script to a list of current employees to determine whether any network accounts were associated with users who were no longer employed by BOCES. We met with the Specialist to review all non-employee network user accounts to determine if any were no longer necessary. We discussed any potential unnecessary network user accounts with BOCES officials.

Our audit also examined the adequacy of certain sensitive 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. The CAP should be posted on the BOCES website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

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