Port Byron Central School District

Network User Accounts

NOVEMBER 2021

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

Contents

Report Highlights

Audit Objective

Determine whether Port Byron Central School District (District) officials ensured network user account controls were secure.

Key Findings

District officials did not ensure that the District's network user account controls were secure.

- District officials did not establish written policies or procedures to add or disable user accounts.

- The District had a total of 19 unneeded network user accounts including 14 non-student accounts, four shared accounts and one generic account.

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

Key Recommendations

- Establish written policies or procedures for managing network user accounts.

- Regularly review network user accounts and disable those that are unnecessary.

- Routinely evaluate shared user accounts and disable those that are no longer needed.

Officials generally agreed with our recommendations and initiated or indicated they plan to initiate corrective action.

Background

The District serves the Towns of Aurelius, Brutus, Conquest, Mentz, Montezuma and Throop in Cayuga County, and the Town of Savannah in Wayne County.

The District is governed by a seven-member Board of Education (Board) responsible for managing and controlling financial and educational affairs.

The Superintendent of Schools is the chief executive officer and responsible for District administration.

The District's Director of Technology (IT Director) is responsible for managing network user accounts.

The District relies on its IT assets for Internet access, email and maintenance of financial, personnel and student records.

Quick Facts

Enabled Network User Accounts	
Student	800
Non-Student	182
Shared	21
Generic	16
Total	1,019

Audit Period

July 1, 2019 – June 30, 2021

Network User Accounts

Network user accounts provide access to network resources and should be actively managed to minimize risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI). 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 individuals or entities.

How Should Officials Manage Network User Accounts?

A school district should have written procedures for granting, changing and revoking access rights to a computerized network. To minimize the risk of unauthorized access, officials should actively manage user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner. To minimize the risk of unauthorized access and misuse, officials should disable unnecessary network accounts as soon as there is no longer a need for them. Former employees' user accounts should be disabled on the day they leave school district employment. Officials also should routinely evaluate generic accounts and disable those that are not related to a current school district or system need.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly and can be created for services that are not linked to a personal account to meet various business needs. A shared network user account is an account with a username and password that is shared among two or more users. Shared accounts are often used to provide network access to guests and temporary or intermittent IT users (e.g., substitute teachers and third-party vendors) and automated processes (e.g., backups and testing). Shared user accounts should be limited to those instances when multiple users must access one computer to perform assigned duties or temporary work, guests, and have expiration date. Because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, each user should have their own user account.

> When user accounts are no longer needed, they should be disabled in a timely manner.

Officials Did Not Establish Written Policies and Procedures to Manage Network User Accounts and Permissions

District officials did not establish written policies or procedures to add or disable network user accounts. The IT Director configured specialized software to automatically add and disable student user accounts on the network and manually managed non-student, shared and generic user accounts. The IT Director was notified of new and departing non-student users by the Assistant Superintendent for Business and Finance.

We examined all 1,019 enabled network user accounts (800 student accounts, 182 nonstudent accounts and 21 shared accounts and 16 generic accounts) to determine whether user accounts were necessary and appropriate. Although there were no formal scheduled procedures for reviewing network user accounts and permissions, we found that student user account additions and deletions were adequately managed using specialized software and non-student user account management could be improved.

Unneeded Non-Student User Accounts – We found 46 of the 182 non-student user accounts for which there was no matching employee record. District officials reviewed these accounts upon our request and it was unclear when officials last performed such a review. Officials indicated they review the accounts on an as needed basis but could not provide documentation when it was last performed. The IT Director told us that 35 of these accounts were for Cayuga-Onondaga Board of Cooperative Educational Services (BOCES) staff or other outside counseling staff who worked or provided services at the District. District staff contacted BOCES and the outside counseling providers for a current listing of employees at the District, which we used to determine that seven of the 35 user accounts were unneeded because the individuals were no longer employed or working at the District. The IT Director told us he disabled the seven accounts.

The IT Director told us that the remaining 11 user accounts belonged to District staff who were not listed on the staff directory for various reasons, such as the School Resource Officer who is paid by voucher. However, the IT Director told us he disabled seven of the 11 user accounts because the employee retired or was no longer employed by the District and the user accounts were no longer needed.

In total the IT Director told us he disabled 14 non-student user accounts that were no longer employed or working at the District. These accounts should have been disabled when the individuals separated employment or service.

Unneeded Generic and Shared User Accounts – Of the 21 shared and 16 generic network user accounts, we found seven shared and three generic user accounts were not used in the last six months. The IT Director reviewed these accounts and told us he disabled three unnecessary shared user accounts and one generic user account because they were no longer needed. The IT Director told us the

District officials did not establish written policies or procedures to add or disable user accounts.

remaining four shared and two generic user accounts were needed because they were used by short-term substitutes or by IT staff for maintenance.

The IT Director told us he disabled one active shared user account created for an outside counseling service because he replaced it with unique user accounts.

Unneeded network user accounts can be potential entry points for attackers because they are not monitored or used and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. When the District has many user accounts that must be managed and reviewed, 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?

The Board should:

1. Adopt written policies and procedures for managing network user accounts, including adding and disabling user accounts.

District officials should:

2. Regularly review and update network user accounts for necessity and appropriateness.

3. Ensure that the IT Director is notified when staff separate employment with the District.

4. Routinely evaluate shared user accounts and disable those that are no longer needed.

THE PORT BYRON CENTRAL SCHOOL DISTRICT
30 Maple Avenue, Port Byron, New York 13140
(315) 776-5728   FAX (315) 776-4050

Michael Jorgensen   **Mitchell C. Toleson**
Superintendent   Assistant Superintendent for Business and Finance

November 3, 2021

Unit Name: Port Byron Central School District
Audit Report Title: Network User Accounts
Audit Report Number: 2021M-119

Audit Response Letter and Corrective Action Plan

Please let the information below serve as the Port Byron Central School District's response to the recent audit conducted by the Office of the New York State Comptroller. The Port Byron Central School District agrees with the key findings and recommendations from the audit and has included the required CAP with this official Audit Response.

Key Findings:

- Port Byron Central School District (PBCSD) officials did not establish written policies or procedures to add or disable user accounts.
- The PBCSD had multiple unneeded network user accounts

Key Recommendations:

1. The PBCSD should establish written policies or procedures for managing network user accounts.
2. The PBCSD should regularly review network user accounts and disable those that are unnecessary
3. The PBCSD should routinely evaluate shared user accounts and disable those that are no longer needed.

Corrective Action Plan:

1. At the November 15, 2021 PBCSD Board of Education meeting, District policy for Data Networks and Security Access was reviewed. A second reading and adoption of policy will be on the agenda at the December 6, 2021 PBCSD Board of Education meeting.
2. The school district has also established written procedures for adding and disabling user accounts. Building administrators and/or department supervisors will submit formal requests to the Director of Technology to create, delete, or make any permission changes to employee network user accounts.
3. The 19 unneeded network user accounts identified in the audit have been deleted.
4. The Director of Technology will perform a quarterly review of all network user accounts and disable any accounts that are unnecessary.

Mission Statement
The community, through the Port Byron Central School, will provide opportunities in a stable and caring environment for students to become literate, life-long learners and pursuers of dreams. We will nurture self-worth and develop personal integrity and social responsibility in our students. Our school will actively involve our community for the betterment of education.

5. All shared user accounts were reviewed and any unnecessary accounts were deleted.
6. The Director of Technology will perform a quarterly review of all shared user accounts and disable any that are no longer needed.

Please review the above CAP and respond if the corrective actions are not satisfactory.

Sincerely,

Michael Jorgensen
Superintendent of Schools
Port Byron Central School District

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.

- We examined network user account and security settings using a specialized audit script. We reviewed the network user 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 followed up with District officials, BOCES officials and outside employers on potentially unneeded accounts.

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.

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.

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.

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. The CAP should be posted on the District's 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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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