REPORT OF EXAMINATION | 2022M-101

Starpoint Central School District

Network Access and Application User Permissions

OCTOBER 2022

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

Contents

Report Highlights

Starpoint Central School District

Audit Objective

Determine whether Starpoint Central School District (District) officials adequately secured access to the network and properly managed user permissions to the financial and student information applications.

Key Findings

District officials did not adequately secure access to the network or properly manage user permissions to the financial and student information applications. In addition to sensitive information technology (IT) control weaknesses that were communicated confidentially to officials, District officials did not:

- Regularly review enabled network user accounts to ensure they were authorized and still needed. As a result, officials did not disable 44 former employee network user accounts. Some of the former employees left the District 13 years ago.
- Limit student information and financial application access rights and permissions based on a user's job responsibilities.

As a result, compromised accounts may not be detected and increased opportunities for users to make unauthorized or improper changes, improperly access students' private and personal information and/or modify accounting records to conceal malicious transactions exist.

Key Recommendations

- Regularly review network user accounts for necessity and appropriateness and disable user accounts when they are not needed.
- Limit access rights and permissions to user's job responsibilities.

District officials generally agreed with our recommendations and indicated that they plan to take corrective action. Appendix B includes our comment on an issue raised in the District's response.

Background

The District serves the Towns of Pendleton, Cambria, Lockport, Wheatfield and Royalton in Niagara County. The Board of Education (Board) is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District has an educational services contract with Orleans/Niagara Board of Cooperative Educational Services (BOCES) that includes providing information technology support through Erie 1 BOCES. The District's network and information systems are managed by the District's Network Manager and the BOCES Coordinator assigned to the District (IT Managers).

Quick Facts	
Student Enrollment	2,900
Employees	387
Total	3,287
Network User Accounts	
Active and Reviewed	3,425
Application Accounts	
Student Information	406
Financial	48
Total Reviewed	454

Audit Period

July 1, 2021 – February 15, 2022

Network Access and Application User Permissions

How Should a School District Adequately Secure Access to the Network and Properly Manage Application User Permissions?

A school board and school district officials are responsible for establishing processes and procedures to secure access to the network and applications by restricting user access to only those network and application resources and data needed for learning or to complete job duties and responsibilities. Network user accounts provide access to resources on a network and are managed centrally by a server such as a domain controller. Application user accounts provide access to resources within each application, such as a financial system or a student information system and are managed by the application. Full direct access to sensitive resources such as operating systems and security software programs should be limited to very few individuals who have a valid business need for such access.

School districts rely on their network for daily business functions such as maintaining their financial and student information applications which contain personnel and student records and data, and for Internet access and email. To minimize the risk of unauthorized network and application access, school district officials should actively manage network and application user accounts, including their creation, use and dormancy, and regularly review them to ensure they are still needed. School district officials should have written procedures in place to grant, change and disable user permissions to the network and specific applications. These procedures should establish who has the authority to grant or change user permissions and allow users to access only what is necessary to complete their job duties. User permissions should be updated as necessary and unneeded accounts should be disabled in a timely manner. School district officials should periodically compare the employee master list to the list of network user accounts to ensure all employee accounts belong to current employees.

School district officials should have written procedures in place to grant, change and disable user permissions to the network and specific applications.

Officials Did Not Disable Unnecessary Network User Accounts

District officials did not adequately secure access to the District's network. District officials did not have a written policy or written procedures establishing a process for adding, modifying or disabling network or application user accounts. In addition, enabled network user accounts were not reviewed to ensure they were authorized and still needed. As a result, the District had unnecessary network user accounts that had not been disabled, including accounts that went unused for periods ranging six months to at least seven years.

We compared all 480 enabled non-student network user accounts to a list of current employees and identified 44 network user accounts that could not be traced to current employees. We determined that these accounts were for former employees who left employment ranging from a period of one month to over 13 years prior, and therefore these network user accounts were unnecessary

and should have been disabled. After we informed District officials about these unnecessary user accounts they were disabled.

We also identified 41 network user accounts that had not been used for periods ranging from six months to at least seven years which included service accounts for administrative functions such as: managing the network, building controls and monitoring, accessing servers and configuring web filtering settings, shared network user accounts and faculty and staff network user accounts. These 41 network user accounts included 18 of the 44 former employee accounts previously mentioned, 14 substitute faculty/staff accounts, eight service accounts and one shared network user account. The 14 substitute faculty/staff network user accounts for individuals who had not worked for the District in at least six months and therefore were unnecessary and should have been disabled, seven of these accounts were never used. After we informed District officials about these unnecessary user accounts they were disabled. The eight service accounts and one shared account, although not having been used in at least six months, were necessary system and/or administrative accounts.

…some employees' accounts remained active up to 13 years after they left the District.

We discussed the 44 former employee network user accounts and the 14 substitute faculty/staff accounts with the IT Managers who told us that these network user accounts had not been disabled because the IT Department was not informed that the employees had separated from the District. The Director of Administrative Services (Administrator) told us that typically the Human Resources Department informed the District Clerk when there were personnel changes. The District Clerk then completed a technology-use request form to request additions and modifications of network user accounts. IT Department staff use the form to add, modify or disable network user accounts, and the Administrator told us that this notification process was overlooked. In addition, this process for adding and disabling network user accounts is not written and detailed in a District policy. The IT Managers told us that one of the former employee accounts had been reassigned to the replacement who needed to access emails and documents for that network user account. However, as of January 2022 the employee had left employment over 260 days prior or almost nine months. Email and document access can be provided without the need to reassign former employees' accounts, as account sharing could compromise user accountability.

Because District officials did not disable unneeded accounts timely or regularly review enabled network user accounts to determine whether they were still needed, some employees' accounts remained active up to 13 years after they left the District. Stale and unneeded network user accounts are additional entry points into a network and, if accessed by an attacker or a former employee, could be used to inappropriately access and view private, personal and sensitive information for malicious purposes. The unneeded accounts were for former teachers and administrative staff, therefore sensitive student and financial information could be inappropriately accessed, modified or deleted if these

accounts were compromised. Additionally, because officials did not monitor network user accounts, compromised accounts may not be detected in a timely manner.

Officials Did Not Properly Manage Application User Permissions

We reviewed all 406 student information application user accounts (19 were assigned to BOCES employees) and all 48 financial application user accounts (15 were assigned to BOCES employees). We found certain user permissions for the student information and financial applications were unneeded to perform the users' job duties.

Student Information Application Permissions – The user permissions granted to employees for the student information application were based on predefined profile templates. We reviewed all 57 permission profiles, and found permissions granted to faculty and staff for the student information system application were appropriate for their job duties. However, permissions granted to five administrative staff (under one permission profile) were more than necessary for their job responsibilities. The application profile template is based on the District's hierarchy rather than job duties. Therefore, all District administrators, such as District office administrators and principals, had the same user permissions including permissions not needed for their specific job duties. For example, one administrator had a student information application user account with full access rights even though access to the student information application was not needed to perform their job duties.

…[P]ermissions granted to five administrative staff (under one permission profile) were more than necessary for their job responsibilities.

The Information/Personnel Coordinator, who is responsible for the student information system application user permissions, told us she uses a profile template for user permissions, and that it was her understanding BOCES was responsible for setting up that template. However, the BOCES Student Information System Coordinator told us that the District is responsible for defining the profile template because the District did not subscribe for these services in its IT services agreement with BOCES. We followed up with the Information/ Personnel Coordinator who told us when she was assigned this position in April 2019, the profiles were already set in the application. She did not realize that she needed to ensure that the profiles were appropriate for each user's job responsibilities when she began in this position.

Financial Application Permissions – The permissions granted to 32 of the 33 District financial application users were appropriate for their job duties. However, one user had full access rights to all modules within the application to add and modify records, which was not needed to perform his job duties.

The administrator who is responsible for the financial system application user permissions told us that due to the small size of the Business Office some of

the application's roles and responsibilities could not be segregated and that the District has adequate compensating controls in place to mitigate the risk of this user's excessive permissions. We reviewed the mitigating controls in place, such as the audit of claims and performing bank reconciliations. Although the controls in place would mitigate some of the risk, officials should add or remove permissions, as needed, for the user's current job responsibilities.

BOCES' User Permissions – We identified 19 student information application user accounts and 15 financial application user accounts assigned to BOCES employees for technical and administrative purposes as an IT services provider. We discussed with BOCES Coordinators the large number of user accounts assigned to BOCES and related access to the student information and financial application. The BOCES Coordinators for both applications told us the user accounts and permissions granted were needed to ensure adequate technical and administrative support was always available to the District when needed. Some of the support staff provide hardware support and other provide administrative support such as assisting employees to generate canned reports or District-tailored reports. Therefore, in general, these user permissions appeared to be reasonable. The BOCES Coordinator for the student information application also told us BOCES was in the process of reviewing access rights granted to their employees and would make appropriate adjustments.

By not properly restricting user permissions within the student information system and financial system applications, there are increased opportunities for users to make unauthorized or improper changes, improperly access students' private and personal information and/or modify accounting records to conceal malicious transactions.

What Do We Recommend?

The Board, District officials and the IT Managers should:

1. Develop and adopt a written user permissions policy and develop comprehensive written procedures detailing the process to add, modify and disable user permissions to the network and applications including identifying the employees responsible for these processes and for notifying the IT Department.

2. Ensure employees responsible for implementing the user permissions policy and procedures are aware of the policy and complying with it.

District officials and the IT Managers should:

3. Periodically evaluate existing network user accounts and disable any unnecessary network user accounts.

4. Disable network user accounts for former employees as soon as these users leave the District.

5. Review student information and financial application user accounts and limit user permissions based on an individual's job duties and to properly segregate duties.

Appendix A: Response From District Officials

STARPOINT
4363 Mapleton Road
Lockport, New York 14094-9652
Central School District

September 26, 2022

Office of the State Comptroller
Melissa A. Myers, Chief Examiner
295 Main Street, Suite 1032
Buffalo, NY 14203-2510

Dear Ms. Myers:

The Starpoint Central School District is in receipt of the New York State Office of Comptroller audit report 2022M-101 entitled *Network Access and Application User Permissions.* Please accept this letter as the District's response to the audit which will be attached and included with the actual audit report published by your office.

On behalf of the Starpoint Central School District's Board of Education and the District's administration, we would like to thank the local field staff who conducted this audit. The District found the staff to be professional and courteous throughout their time at Starpoint.

The Starpoint Central School District appreciates that your audit confirms that the District's technology team has provided our staff and students with secure, safe, and reliable technology and that our technology infrastructure is constantly monitored and safeguarded to ensure the viability of the systems.

See Note 1 Page 8

The Starpoint Central School District appreciates the extensive audit that was performed by the State Comptroller's Office and that the suggestions for improvement offered by the State Comptroller's Office will be addressed by District staff and administration. The District will prepare the required corrective action plan and have the plan officially approved by the Starpoint Board of Education prior to the statutory required date.

Respectfully submitted,

Dr. Sean Croft
Superintendent of Schools

Appendix B: OSC Comment on the District's Response

Note 1

While we appreciate the District's position regarding the safety, security and reliability of the District's technology system, District officials did not adequately secure access to the network or properly manage user permissions to the financial and student information applications. Our report has identified opportunities to improve internal controls over the District's network and to make student and financial information more secure.

Appendix C: 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 interviewed District officials, employees and BOCES personnel and reviewed the District's policy manual to determine the policies in place and to gain an understanding of IT operations, specifically those related to the granting, modifying and revoking of network user accounts and user permissions for the student information system and financial system applications.
- We provided the IT Managers with a computerized audit script to run on the domain controller on November 15, 2021. We analyzed each report generated by the script to identify network user accounts and security settings that indicated ineffective IT controls.
- We compared the employee master file report to the names of all account users listed in the audit script report to determine whether all users with enabled network user accounts were currently employed by the District.
- We reviewed user permissions reports for the student information system and financial system applications to determine how user permissions were managed. For all user accounts, we examined the user permissions and discussed with District officials to determine whether access was necessary and appropriate based on job duties.

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.

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.

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 D: 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

BUFFALO REGIONAL OFFICE – Melissa A. Myers, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

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