REPORT OF EXAMINATION | 2021M-148

Springville-Griffith Institute Central School District

Access to Network and Information Applications

JANUARY 2022

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

Contents

Report Highlights

Springville-Griffith Institute Central School District

Audit Objective

Determine whether Springville-Griffith Institute Central School District (District) officials adequately secured access to the network, student information and financial applications.

Key Findings

Although District officials restricted access to the student information application, they did not adequately secure access to the network and financial application. District officials did not:

- Disable unnecessary generic network user accounts.
- Properly restrict user permissions in the financial application.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Review generic network user accounts and ensure that unnecessary accounts are disabled.
- Review financial application user accounts and limit access rights and permissions based on a user's job responsibilities and to properly segregate duties.

District officials agreed with our findings and recommendations and indicated that they planned to take corrective action.

Background

The District serves the Towns of Aurora, Boston, Colden, Collins, Concord and Sardinia in Erie County and the Towns of Ashford, East Otto and Yorkshire in Cattaraugus County.

The District is governed by an elected seven-member Board of Education (Board). The Board 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 District's day-to-day management under the Board's direction.

The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records and data. The District employs a Director of Technology, Data and Assessment (Director) to manage its IT department.

Quick Facts	
Student Enrollment	1,647
Employees	566
Network Accounts	
Student	1,551
Employee	342
Generic	338
Other	12
Total	2,243

Audit Period

July 1, 2020 – August 13, 2021. We extended our scope period back to the summer of 2019 before the COVID-19 pandemic to verify whether District officials reviewed network accounts.

Access to the Network and Information Applications

User accounts identify specific users and accounts. Network user accounts provide access to resources on a network[1] and are managed centrally by a server computer and/or domain controller.[2] Application user accounts provide users with access to resources within each information application, such as a financial application or a student information application and are managed by the application server.[3]

How Should District Officials Secure Access to the Network and Information Applications?

To minimize the risk of unauthorized network and application access, the Director should actively manage network and application user accounts and periodically conduct a user account review and any account that cannot be associated with an authorized user or current District need should be disabled.

Officials should have written procedures in place to grant, change and disable user permissions to the network and 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.

Because generic 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, all users should have and use their own user account to gain access to a network and applications. If generic accounts are needed, officials should have procedures in place to monitor who uses the accounts and when they are used.

The Director should set up user accounts with specific user permissions needed by each individual to perform their job functions. Properly assigned user access rights, based on the requirements of an individual's job responsibilities, help to preserve an appropriate segregation of duties within the network and applications. The Business Administrator should periodically review user permissions in the financial application to ensure permissions are appropriate and properly limited based on each user's current job roles and responsibilities.

---

1 A network is a group of two or more connected computers. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application.

2 A server is a computer equipped with specific programs that provide resources and data to other computers which are connected to the server. A domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

3 An application server is a program on a server computer that handles all application operations between users and an organization's back-end applications or databases. The front-end is the user interface, typically web-based, where users input information and make information requests. The back-end is the application and database on the server that delivers information to users.

Access to the Network and Financial Application Was Not Properly Restricted

Although District officials restricted access to the student information application, they did not adequately secure access to the network and financial application. The District has written procedures for granting, changing and disabling user permissions to the network and applications. According these procedures, the Director has the authority to grant or change user permissions and should review access rights and permissions at least annually in September and October.

Generic Network User Accounts – During our review of all 2,243 network accounts, we found 338 generic network user accounts that had varied purposes ranging from administrative functions such as building controls, instructional purposes such as accounts for students to share and accounts used to access servers and configure web filtering settings. Because there was such a large number of generic accounts, officials could have difficulty managing them and identifying their uses to determine their necessity.

The Director deleted 65 and disabled 41 generic network user accounts after we brought this to her attention because the accounts were no longer necessary.[4] She told us that the District usually reviewed network accounts during the summer, but during the COVID-19 pandemic, her priority had been to provide support for remote and hybrid-learning. However, we found 21 generic network user accounts had a last logon date prior to July 2019 and had not been disabled prior to the pandemic during the summer of 2019.

Because the Director was not implementing District procedures to review generic accounts, the District is exposed to a greater risk that personal, private and sensitive information (PPSI)[5] could be changed intentionally or unintentionally or be used inappropriately, and officials may not be able to identify who performed the unauthorized activities.

Unneeded Application User Accounts and Permissions – During our review of all 85 user accounts in the District's financial application, we found six unnecessary BOCES[6] support service user accounts which were disabled after we informed District officials. Unnecessary user accounts that have not been disabled could potentially be used by former employees or others for malicious purposes.

4 The remaining shared accounts were necessary for District operations and being used by various software applications.

5 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.

6 Board of Cooperative Educational Services

Of the 79 user accounts, we selected and reviewed all five Business Office employees' user accounts permissions in the District's financial application. We found that all five users had unnecessary permissions and one user had administrative access rights. By not properly restricting user permissions and access rights within the financial application, there is increased opportunities for users to make unauthorized or improper changes and modify the accounting records to conceal the transaction.

Officials told us that due to the small size of the Business Office, users were cross-trained on other job functions and therefore required more permissions than necessary for their daily job responsibilities. However, officials could add and remove employees' access rights as needed and could always enable certain permissions when necessary (e.g., during an employee's extended absence) and mitigate risks.

Because officials did not adequately secure access to the network and financial application, the District has a greater risk that its network resources and financial data could be changed intentionally or unintentionally or be used inappropriately.

What Do We Recommend?

District officials should:

1. Periodically review user accounts and ensure that unnecessary generic network user accounts are disabled, as required by its written procedures.
2. Review financial application user accounts and limit access rights and permissions based on a user's job responsibilities and to properly segregate duties, as also required by its written procedures.
3. Assign the responsibilities of financial application administrator to the Director or other designated employee who is not involved in the District's financial operations.

Appendix A: Response From District Officials

SPRINGVILLE-GRIFFITH INSTITUTE CENTRAL SCHOOL DISTRICT
VISION: A PLACE WHERE EVERYONE FINDS VALUE AND MEANING EVERY DAY
www.springvillegi.org
267 Newman Street • Springville, New York 14141-1599 • FAX (716) 592-3209

Kimberly Moritz
Superintendent of Schools
716-592-3230
kmoritz@springvillegi.org

Kathy Tucker
Secretary, District Clerk
716-592-3230
ktucker@springvillegi.org

December 24, 2021

Office of the New York State Comptroller
Division of Local Government & School Accountability
PSU - CAP Submission
110 State Street, 12th Floor
Albany, NY 12236

The Office of the State Comptroller completed an audit of the school district's access to network and information applications between July 1, 2020 - August 13, 2021. Representatives from our school district had the opportunity to review these recommendations with members of the Comptroller's office on December 10, 2021. The draft audit revealed the following two key recommendations:

- Review generic network user accounts and ensure that unnecessary accounts are disabled.
- Review financial application user accounts and limit access rights and permissions based on a user's job responsibilities and to properly segregate duties.

Please let the information below serve as the Springville-Griffith Institute Central School District's response to the recent audit. The areas in which the district was cited for improvement are addressed below with corrective actions included. The Springville-Griffith Institute Central School District is in agreement with the findings and has combined the Comprehensive Action Plan (CAP) with the Audit Response Letter. The findings from this audit will help our district to improve its information technology systems.

Recommendation:

- Review generic network user accounts and ensure that unnecessary accounts are disabled.

Corrective Action Plan:

1. The district technology staff reviewed the 338 generic accounts and identified the following:
    a. 113 accounts are used for entry/exit ID card door access. These accounts have no access to the district's network.
    b. The district consolidated an additional 106 program-based accounts.
    c. The remaining necessary generic accounts are documented in regard to their purpose and need.
2. The district will periodically conduct a review of user and network accounts and any account that is associated with an authorized user or current school district need will be disabled.
3. If generic accounts are needed, the district will document accounts for their purpose and need.

Springville-Griffith Institute Central School District Mission: We are a learning community that cultivates meaningful relationships, commits to growth and improvements, says "YES" to voice, choice and creativity, and knows learning is limitless.

Recommendation:

- Review financial application user accounts and limit access rights and permissions based on a user's job responsibilities and to properly segregate duties.

Corrective Action Plan:

1. Upon further review an additional five accounts were disabled.
2. The district has completed a comprehensive review of all users' rights and permissions. Accounts will be assigned by user access rights, based on the requirements of an individual's job responsibilities.
3. The district will periodically conduct a review of user accounts and remove any unnecessary rights and permissions. Permissions will be updated as necessary and unneeded accounts will be disabled in a timely manner.
4. The responsibility of the financial application will be assigned to a designated employee who is not involved in the district's financial operations.

The Board of Education, Superintendent, Business Official and Director of Technology appreciate the findings of this report and will consider the Comptroller's recommendations as we move forward.

Sincerely,

Kimberly Moritz
Superintendent of Schools

Alllson Duwe
SGI BOE President

Springville-Griffith Institute Central School District Mission: We are a learning community that cultivates meaningful relationships, commits to growth and improvements, says "YES" to voice, choice and creativity, and knows learning is limitless.

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 our audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and reviewed Board policies, regulations and minutes to gain an understanding of the District's policies, procedures, network and related IT controls.
- We provided a computerized audit script to the Director to run on the domain controller[7] on June 1st and June 2nd, 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 District's current student enrollment list and master payroll list to the network user accounts identified by the scripts to determine whether active network account users were either enrolled students or District employees.
- Using various software permission reports from the financial application, we determined how user permissions were managed. We examined the user permissions for all five Business Office employees to determine whether access to the financial application was appropriate based on their job duties.
- We reviewed access granted to the student information application and determined if the access is appropriate based on the employees' job titles or students' status.

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 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.

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.

7 The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain. It is responsible for allowing users to access network resources.

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.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