REPORT OF EXAMINATION | 2021M-118

Bainbridge-Guilford Central School District

Network User Accounts

OCTOBER 2021

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

Contents

Report Highlights

Bainbridge-Guilford Central School District

Audit Objective

Determine whether Bainbridge-Guilford Central School District (District) officials adequately managed network user accounts.

Key Findings

District officials:

- Did not adequately manage network user accounts. We identified 66 unneeded user accounts including 52 generic accounts and 14 former employees' accounts.
- Adequately managed network administrative permissions.

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

Key Recommendations

- Disable former employees' network user accounts as soon as they leave District employment.
- Periodically evaluate existing network user accounts, including generic accounts and disable any deemed unneeded.

District officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The District serves the Towns of Sanford in Broome County, Afton, Bainbridge, Coventry, Guilford, Norwich and Oxford in Chenango County, Masonville and Sidney in Delaware County, and Unadilla in Otsego County.

The District is governed by an elected 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 contracts with the South Central Regional Information Center (SCRIC) to provide IT services, which includes an IT Coordinator, who, in part with the Superintendent, manages the network user accounts and permissions.

Quick Facts	
Student Network Accounts	938
Nonstudent Network Accounts	296
Employees	270

Audit Period

July 1, 2019 – April 22, 2021

Network User Accounts

Why Should Officials Monitor Network User Accounts and Permissions?

Network user accounts provide users with 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)[1], make changes to employee or student records or deny access to electronic information.

To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions, 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. A district should have written policies and procedures for granting, changing and removing user access and permissions to the network.

Generally, an administrative account has permissions to monitor and control a network, computers and applications that can include adding new users and changing user passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, officials must limit administrative permissions to only those users who need them to complete their job functions.

We found 66 of the user accounts were unneeded…

Officials Did Not Adequately Manage Network User Accounts

The Board adopted a policy that provides for managing user accounts and permissions and the periodic review of user accounts. However, there are no specific procedures for granting, changing and removing user access and permissions.

The District uses a software platform to assist in the management of user accounts. Ten individuals are authorized to request new staff accounts. These requests go to the SCRIC employees who would then set up the accounts. The Business Office staff review the user account list annually for any unknown individuals and will let the IT Coordinator know if there are any accounts that should be deleted. We reviewed all 296 enabled nonstudent network user accounts to determine whether any were unneeded.

We found 66 of the user accounts were unneeded and could be disabled, including 52 generic accounts and 14 former employees' accounts. Although

1 Personal, private and sensitive information (PPSI) is any information where authorized 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.

business office staff review the user account list annually, employees leave District service throughout the year and their accounts may not be disabled timely. Also, the business office staff would not be able to identify whether generic accounts should be disabled since these accounts are not assigned to a specific individual and are sometimes created to run certain network services. Therefore, the District had unneeded and unused network user accounts that were not disabled. The IT Coordinator told us these accounts would be deleted.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view student or employee PPSI and the risk increases that this PPSI could be changed intentionally or unintentionally or used inappropriately.

Officials Adequately Managed Network Administrative Permissions

Four individuals are authorized to request changes to network user accounts' permissions. These requests go to the SCRIC employees who would then change the account permissions. We reviewed the 296 enabled nonstudent network user accounts to determine whether any had unneeded administrative permissions.

We found two network user accounts with administrative permissions, which were deemed necessary. SCRIC employees use these two accounts for account management or to track changes within the account management software and files.

Adequately managing the network administrative permissions strengthens a network since a compromised network administrative account has elevated privileges and could be used by an attacker to cause greater damage than a lesser-privileged account, including unauthorized manipulation of data or disruption of District operations.

Adequately managing the network administrative permissions strengthens a network…

What Do We Recommend?

District officials should consider revising their current written procedures to include:

1. Granting, changing and removing user access and permissions.
2. Disabling former employees' network user accounts as soon as they leave District employment.
3. Assigning the periodic review of the existing network user accounts list to someone with knowledge of generic accounts and disable any deemed unneeded.

Appendix A: Response From District Officials

BAINBRIDGE-GUILFORD CENTRAL SCHOOL DISTRICT
18 JULIAND STREET — BAINBRIDGE, NEW YORK 13733-1097

Jr.-Sr. High School (607) 967-6300
Telefax (607) 967-4231
Guilford Elementary School (607) 895-6700
Administrative Offices (607) 967-6321
Business Offices (607) 967-6335
Greenlawn Elementary School (607) 967-6301

September 28, 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

To whom it may concern:

Please let the information below serve as the Bainbridge-Guilford Central School District's response to the recent technology audit. The areas in which the district were cited for improvement are addressed below with corrective actions included. The Bainbridge-Guilford Central School District is in agreement with the findings and have combined the CAP with the Audit Response Letter.

Summary of Findings:

- User accounts were not adequately managed

Recommendations:

- Granting, changing and removing user access and permissions. DISTRICT AGREES
- Disabling former employees' network user accounts as soon as they leave district employment. DISTRICT AGREES
- Assigning the periodic review of the existing network user accounts list to someone with knowledge of generic accounts and disable any deemed unneeded. DISTRICT AGREES

Corrective Action Plan:

1. The district has a small team of authorized staff members who have district approval to make any changes or additions to employee network accounts. These authorized requestors will be tasked with submitting support tickets to the SCRIC Service Desk to create, delete or make any access or permission changes to employee network user accounts.

2. The district utilizes an employee exit form with a checklist to ensure any network user access is removed as soon as they leave the district. An authorized district requestor will submit a support ticket with the SCRIC Service Desk to have the network user account disabled on the date of exit. Any employee who is terminated will have their network user account disabled immediately per an authorized district requestor support ticket with the SCRIC Service Desk.

3. The district will assign a review of existing network user accounts at least once annually to determine if the accounts should remain active or be deleted. This process will also include a district and IT department review of any district created generic accounts to determine if they are still needed. Any account deemed unneeded will be deleted per an authorized district requestor support ticket made to the SCRIC Service Desk.

Please let me know if the enclosed corrective actions are not satisfactory. The Bainbridge-Guilford Central School District will implement all recommendations via our Technology Department and our Technology Team. Thank you for working with the district throughout this process. We have learned a great deal.

Sincerely,

Timothy R. Ryan
Superintendent of Schools

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 interviewed District officials and reviewed the District's IT related policies and procedures to gain an understanding of the IT environment and internal controls, specifically those related to granting, modifying and disabling network user accounts and permissions.
- We used specialized audit software to examine the District's domain controller and analyzed the data produced to assess network user accounts, permissions assigned to the accounts and the related security settings applied to the accounts. We compared 296 nonstudent network user accounts to the active employee list to identify accounts for former employees and/or unneeded accounts. We reviewed automated settings to identify any settings that indicated ineffective IT controls.
- We followed up with District officials on potentially unneeded accounts and automated settings that indicated ineffective controls.

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 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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins counties

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