REPORT OF EXAMINATION | 2021M-84

Haldane Central School District

Information Technology

NOVEMBER 2021

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

Contents

Report Highlights

Haldane Central School District

Audit Objective

Determine whether Haldane Central School District (District) officials adequately managed and monitored user accounts and permissions.

Key Findings

District officials did not adequately manage and monitor user accounts and permissions. As a result, the District has an increased risk that it could lose important data and suffer serious interruption in operations. District officials did not:

- Disable 74 unneeded network user accounts of the 300 accounts we examined. The 74 accounts included generic and former employee accounts.
- Create secondary user accounts, for three network user accounts with administrative permissions, to be used for non-administrative activities.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Evaluate all network user accounts to ensure unneeded network user accounts are disabled.
- Assess all network user accounts with administrative permissions and create secondary accounts to be used for non-administrative activities.

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

Background

The District serves the Towns of Phillipstown in Putnam County and Fishkill in Dutchess County.

The District is governed by an elected five-member Board of Education (Board) responsible for the general management and control of financial affairs. The Superintendent of Schools is the chief executive officer responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The District contracts for onsite information technology services (consultants). The District's Information Technology Specialist (IT Specialist) is responsible for managing the District's IT assets including network security and user accounts. The consultants support the IT Specialist in her duties.

The District relies on its IT assets for Internet access, email and maintaining confidential and sensitive financial, student and personnel records.

Quick Facts

Network User Accounts	
Students	858
Non-Students	300
Total	1,158
Employees	277
Student Enrollment	821

Audit Period

July 1, 2019 – November 30, 2020

We expanded our audit period forward through March 18, 2021 to review user accounts.

User Accounts

Why Should Officials Manage Network User Accounts and Permissions?

District officials are responsible for restricting network user access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets are secure from unauthorized use and/or modification.

Network user accounts provide users with access to network resources and should be actively managed to minimize the 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 the records or deny access to electronic information.

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

Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Officials should routinely evaluate generic network user accounts and disable those that are not related to a system need.

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

Officials Did Not Adequately Manage Network User Accounts and Permissions

District officials did not adequately manage user accounts and permissions for the District's network. Officials did not have written procedures for managing user accounts and permissions.

1 PPSI is any information to which unauthorized access, disclosure, modification or destruction – 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.

Officials told us that when an employee was hired or terminated, the building principal or District office staff send an email to the IT Specialist, authorizing her to grant, modify or disable the employee's user account. However, this procedure was not always followed, resulting in unneeded network user accounts and administrative accounts used for non-administrative tasks that went unnoticed until our audit.

We examined all 300 non-student network user accounts to determine whether any were unneeded or had unneeded administrative permissions.

Unneeded Network User Accounts – We found 74 network user accounts were unneeded and could be disabled, including 39 generic network user accounts and 35 non-student network user accounts.

The generic network user accounts included several service accounts previously used to manage computer processes and test accounts used to check how well the web filtering program was working. While these generic network user accounts may have been used in the past most have not been used in more than six months and are no longer needed.

Three network administrators did not have separate, lesser-privileged accounts for non-administrative functions....

Of the 35 non-student network accounts, 11 accounts had not been used for more than two years, 10 were last accessed between July 4, 2019 and June 22, 2020, 12 had never been used to log into the network and two accounts were for users who are no longer employed by the District. Although we did not review student network accounts, the IT Specialist told us some of these accounts were service accounts or student accounts used by teachers to review student work. She said she would disable all the 74 unneeded non-student network user accounts we identified.

If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. 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.

Unnecessary Administrative Permissions – Three network administrators did not have separate, lesser-privileged accounts to be used for non-administrative functions, such as browsing the Internet and checking email. The IT Specialist told us she was unaware these users needed separate, lesser-privileged accounts and will have their accounts set up properly with lesser-privileged accounts for non-administrative duties.

Without assigning and providing a separate non-administrative network user account for routine activities that do not require administrative permissions, the District is at a significantly greater risk of unauthorized access and loss of resources including PPSI.

When users have unneeded administrative permissions to networks and computers, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

Why Should District Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data. In addition, the training should communicate related policies and procedures to all employees.

The training should center on emerging trends such as information theft, social engineering attacks and computer viruses and other types of malicious software, all of which may result in PPSI compromise or denying access to the IT system and its data. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything attendees need to perform their jobs.

Also, the training should cover key security concepts such as the dangers of Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training...

Not All IT Users Received IT Security Awareness Training

District officials did not ensure all users received IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets. Although the IT Specialist provided some training during our audit period, not all employees attended, and no records were available showing the kind of training provided. As a result, we could not determine whether the IT training provided was adequate.

The IT Specialist told us that they are in the process of incorporating information security awareness training into their global safety network training modules as part of the mandatory trainings to be taken by all employees. However, we did not find any evidence that this was happening.

Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, District data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

District officials should:

1. Develop and adhere to written procedures for granting, changing and disabling network user account access.
2. Disable network user accounts of former employees as soon as they leave District employment, periodically evaluate existing network user accounts including generic and student accounts and disable any deemed unneeded.
3. Ensure that all users with administrative account access use a dedicated or secondary account for non-elevated activities.
4. Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use.

Appendix A: Response From District Officials

HALDANE
CENTRAL SCHOOL
DISTRICT

October 19, 2021

Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

The Office of the State Comptroller completed an audit of the school district's information technology systems between July 1, 2019 and March 18, 2021. The draft audit revealed two key recommendations, including:

- Evaluate all network user accounts to ensure unneeded network user accounts are disabled.
- Assess all network user accounts with administrative permissions and create secondary accounts to be used for non-administrative activities.

Representatives from our school district had the opportunity to review these recommendations with members of the Comptroller's office on September 23, 2021. At this meeting the district requested that the auditor share their record of unneeded network user accounts that were cited in the draft audit report (74 cited accounts) as it was discrepant from the district's records (67 accounts). The auditor provided this information and our school district was able to reconcile this discrepancy.

There is no additional information that the district seeks to be clarified and/or included prior to the final report as the district agrees with the findings and recommendations. Our staff has appreciated the time to work with the Comptroller's office through this audit period.

Sincerely,

Phil Benante

Phil Benante, Ed. D.
Superintendent of Schools

cc: Haldane Central School District Board of Education Members
Anne Dinio, School Business Official

HALDANE CENTRAL SCHOOL DISTRICT 15 CRAIGSIDE DRIVE • COLD SPRING, NY 10516 • 845.265.9254

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 to gain an understanding of the IT environment and internal controls.
- We used our professional judgment to select a sample of five District computers assigned to five employees from the District's 140 desktop computers. We selected computers of users who had access to PPSI. We examined these computers using specialized audit script to determine whether user accounts had administrative permissions.
- We used specialized audit script to examine the District's domain controller[2] 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 the 300 non-student network accounts to the active employee list to identify accounts for former employees and/or unneeded accounts.
- We inquired with District officials regarding whether they received along with District personnel IT security awareness training.

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.

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.

2 A Microsoft server that runs Active Directory and controls or manages access to 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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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