New York State Comptroller
THOMAS P. DiNAPOLI

Hilton Central School District

Network Access Controls

2022M-200 | June 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Hilton Central School District

Audit Objective

Determine whether Hilton Central School District (District) officials ensured network access controls were adequate.

Key Findings

District officials did not ensure that network access controls were adequate. As a result, data and personal, private and sensitive information (PPSI) are at greater risk for unauthorized access, misuse or loss. In addition to sensitive network access control weaknesses that we confidentially communicated to officials, we found that:

- District officials did not establish written policies or adequate written procedures for managing network user account access, including adding or disabling user accounts and permissions.
- The District had 230 unneeded enabled network user accounts, including those for former students, former employees and others who were no longer providing services to the District.

Key Recommendations

- Establish adequate written policies and procedures for managing network user account access.
- Regularly review network user accounts and disable unneeded accounts in a timely manner.

District officials agreed with our findings and indicated they have initiated corrective action.

Background

The District serves the Towns of Clarkson, Greece, Hamlin and Parma in Monroe County.

The District is governed by a seven-member Board of Education (Board) that is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for District administration.

The District's Director of Technology (IT Director) is responsible for managing information technology (IT) operations, including network access controls, with assistance from the network administrator and other technology department staff. The IT Director started at the District effective February 28, 2022.

Quick Facts

Enabled Network User Accounts	
Student	4,119
Individual Nonstudent	1,033
Service	126
Shared	27
Total	5,305

Audit Period

July 1, 2020 – October 26, 2022

Network Access Controls

A school district relies on its network for maintaining financial, student and personnel records and Internet access and email, much of which contain 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.

If a school district's network access is compromised or disrupted, the results could range from inconvenience to significant damage and could require extensive effort and resources to evaluate, repair and/or rebuild. While effective network access controls will not guarantee the safety of these systems, without these controls, a school district has an increased risk that its network hardware and data contained therein, including PPSI, may be exposed, damaged or lost through inappropriate access and use.

If a school district's network access is compromised or disrupted, the results could range from inconvenience to significant damage. …

How Should Officials Control User Account Access to the Network?

School district officials are responsible for restricting network user account access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and information technology (IT) assets accessible by network user accounts are secure from unauthorized use, access and/or loss. School district officials should develop written policies and procedures for managing network user account access including adding and disabling user accounts.

A service account runs a particular network or system service or application (e.g., backups). Service accounts may not be authorized or monitored by an individual and, therefore, may have reduced accountability. Shared user accounts have a username and password that are shared among two or more users and are used, for example, to provide access to guests and other temporary or intermittent users. Because shared accounts are not assigned to an individual user, accountability may be reduced and officials may have difficulty managing them and linking suspicious activity to a specific user.

Unneeded user accounts are additional entry points into the school district's network. If accessed by unauthorized users, they could be used to inappropriately access the school district's network to review and/or remove personal information; make unauthorized changes to school district records; or deny legitimate access to the school district's network and records. Therefore, officials should disable unneeded user accounts as soon as they are no longer needed and regularly monitor network user accounts to ensure they are appropriate and authorized.

Officials Did Not Adequately Control User Access to the Network

District officials did not adequately manage network user account access. The District appropriately granted administrative permissions but had unneeded network user accounts that were not disabled or monitored. Upon our inquiry, the network administrator disabled 230 network accounts that were no longer necessary.

Specifically, the network administrator disabled 184 individual (112 student, 72 nonstudent), 36 service and 10 shared network user accounts because they were not necessary (Figure 1). Overall, 4 percent of the 5,152 individual user accounts and 30 percent of the 153 service and shared network user accounts were not needed. The disabled user accounts included those for former employees or other individuals who no longer provided services to the District, former students or duplicate user accounts that were not needed. The network administrator did not provide an adequate explanation as to why the accounts were not previously disabled. Additionally, five more user accounts were assigned to seasonal employees or employees on long-term leave that should have been temporarily disabled and re-enabled when needed.

Figure 1: Unnecessary Network User Accounts

	Total	Unnecessary	
Network User Accounts Assigned to Individuals			
Students	4,119	112	3%
Nonstudents	1,033	72	7%
Total	**5,152**	**184**	**4%**
Other Network User Accounts			
Service	126	36	29%
Shared	27	10	37%
Total	**153**	**46**	**30%**

These accounts should have been disabled as soon as they were no longer needed, such as when the individuals transferred, graduated, left District employment or stopped providing services to the District. However, they remained enabled for much longer than necessary. For example, we identified nine enabled user accounts of former employees who had not been employed by the District, and had not used their user accounts, in more than two years.

Network access controls were not secure and adequately managed because District officials did not develop adequate written policies or procedures for adding and disabling network user accounts.

[W]e identified nine enabled user accounts of former employees who had not been employed by the District, and had not used their user accounts, in more than two years.

The Superintendent told us that they were working on developing a written policy and procedures but were delayed by staff turnover, such as the current IT Director starting in February 2022. However, District officials should have previously developed written policies and procedures, which would have helped provide guidance when turnover occurred. The IT department had written internal department procedures that consisted of a table indicating which non-full-time staff positions were allowed to have network access. The procedures indicated that certain positions, including per diem substitutes and coaches, were not allowed individual network user accounts unless there was a request from human resources or the athletic director (for coaches). However, the procedures were inadequate because they did not include guidance for reviewing, adding or disabling network user accounts or permissions.

District officials could not provide a documented request to provide network access for 24 coaches and per diem substitutes. The IT Director told us that 10 of the coaches were provided network access to comply with documentation requirements during the COVID-19 pandemic, and two of the substitutes were in positions that were allowed to have access. However, District procedures did not appropriately distinguish between different substitute positions. The IT Director did not provide an explanation for the other 12 user accounts.

The IT Director and network administrator implemented an automated process for adding and disabling non-temporary employee user accounts in September 2022 so that the employee's user account with certain permissions will be added or disabled when the employee's record becomes active or inactive in the human resources software. Also, they started adding termination dates for non-employee user accounts (when known, or no more than one year) so that the account will be disabled at a specific date and they will have the option to re-enable the user account if access is needed beyond that date.

Furthermore, on December 16, 2022, after the conclusion of fieldwork, the IT Director provided updated written IT department procedures. They included an updated table of which positions were allowed network access, more detailed procedures for how those accounts will be added, and required an annual audit of all 'active' (i.e., enabled) user accounts be performed in conjunction with human resources.

The unneeded network user accounts were additional entry points into the District's network. As a result, PPSI was at greater risk for unauthorized access, misuse or loss. We encourage District officials to continue improving their procedures and controls over network user accounts to help secure network access.

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a written network user account access policy and ensure IT department staff develop adequate written supplemental procedures that define the circumstances in which access should be revoked (e.g., termination, retirement, graduation, end of contract), as well as a maximum timeframe for IT staff to complete that process once those conditions have been met.

The IT Director should ensure:

2. Written network user account access procedures are updated to meet current District needs, and that staff comply with the written procedures and maintain documentation for necessary network user account requests and approvals.

3. Staff disable unneeded network user accounts in a timely manner and regularly review and update user accounts and permissions.

Appendix A: Response From District Officials

HILTON CENTRAL SCHOOL DISTRICT
SUPERINTENDENT'S OFFICE
225 WEST AVENUE • HILTON, NY 14468
585.392.1000 • FAX: 585.392.1038
WWW.HILTON.K12.NY.US

Casey Kosiorek, Ed.D.
Superintendent of Schools
Ext. 7043

April 19, 2023

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller, Rochester Regional Office
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608

Dear Mr. Grant:

The Hilton Central School District has received and reviewed the draft Report of Examination entitled Network Access Controls for the period covered July 1, 2020 – October 26, 2022. On behalf of the Board of Education and administration, we appreciate the opportunity to respond to the findings and to provide our responses to the audit recommendations.

During the course of the audit, the Comptroller's Office conducted a comprehensive examination of the District's information technology (IT) network access controls. We appreciate the courteous and professional manner in which the auditors worked with us during the audit as well as the thoroughness of their audit procedures.

The Hilton Central School district is working to continuously review and improve our security posture. We currently work with an outside cyber security vendor to evaluate our systems and practices against best practices and industry standards, in addition to State Guidelines and Ed Law 2-d requirements. We agree with your finding and are working diligently to implement changes in documentation, processes and system configurations in order to safeguard our network and data against Cyber threats. Additionally, Hilton CSD has recently proposed the hiring of a full-time, dedicated cyber security employee. This proposed additional employee will allow for dedicated resources and expertise in the cyber security space.

A separate corrective action plan will be submitted as outlined in the Office of the New York State Comptroller's guidance document titled Responding to an OSC Audit Report: Audit Responses and Corrective Action Plans.

Again, the Hilton Central School District expresses gratitude for the examiners and the work they performed as part of the examination. The Board, Superintendent, Director of Technology, and information technology staff will continue to maintain controls and accountability over information technology network access controls.

Sincerely,

Casey Kosiorek, Ed.D.
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 reviewed the District's IT policies and procedures and interviewed District officials and staff to gain an understanding of IT operations and controls, specifically those related to network access controls.
- We examined network user accounts and administrative permissions using a computerized audit script run on May 3, 2022. We reviewed network user accounts and compared them to current employee and student lists to identify unused and other possibly unneeded network user accounts and permissions.
- We reviewed network user accounts for coaches and per diem substitutes to determine whether they had the required approvals for network access.
- We inquired with District officials and staff about possible unneeded network user accounts and permissions.

Our audit also examined the adequacy of certain sensitive network access 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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

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, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties