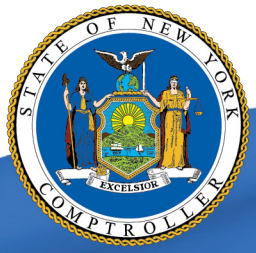
REPORT OF EXAMINATION | 2021M-127

Horseheads Central School District

Network Access Controls

NOVEMBER 2021



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

Contents

Report Highlights

Horseheads Central School District

Audit Objective

Determine whether Horseheads Central School District (District) officials ensured network access controls were secure.

Key Findings

District officials did not ensure that the District's network access controls were secure. Officials:

- Paid BOCES more than $2 million in the 2019-20 fiscal year for IT services but did not enter into a service level agreement (SLA) to clearly identify BOCES responsibilities and services to be provided. As a result, officials were unable to determine exactly what services they paid for, if the District was appropriately billed or receiving the best value for IT services.
- Did not establish formal policies or procedures to add or disable user accounts. As a result, there were 230 inactive user accounts, of which 138 were unneeded, and there were an excessive number of generic accounts.
- Did not provide IT security awareness training to employees.

Key Recommendations

- Regularly review network user accounts and disable those that are unnecessary.
- Develop an SLA to address the District's specific needs and expectations for IT services.
- Ensure that officials and employees receive adequate IT security awareness training.

District officials partially agreed with our recommendations. Appendix B includes our comments on issues raised in the District's response.

Background

The District serves the Towns of Horseheads, Big Flats, Catlin, Erin, and Veteran in Chemung County and the Town of Cayuta in Schuyler County.

The District is governed by a nine-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's IT Manager oversees day-to-day IT operations. Greater Southern Tier Board of Cooperative Educational Services (BOCES) provides computer technicians and IT services to assist with these duties.

The District relies on its IT assets for Internet access, email and the maintenance of financial, personnel and student records.

Quick Facts

Enabled Network User Accounts	
Student	3,745
Generic	83
Staff	893
Total	**4,721**

Audit Period

July 1, 2019 – August 11, 2021

Network Access Controls

Why Should Officials Manage Network User Accounts and Permissions?

Network user accounts provide users with access to network resources based on assigned permissions 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 records or deny access to electronic information.

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

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

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. A shared network user account is an account with a username and password that is shared among two or more people. Shared accounts are often used to provide access to guests and temporary or intermittent IT users (e.g., substitute teachers and third-party vendors) and automated processes (e.g., backups and testing).

Officials Did Not Adopt Policies and Procedures to Manage Network User Accounts and Permissions

District officials did not establish formal policies or procedures to add or disable user accounts but are currently developing them. Since July 1, 2019, the IT Director was responsible for completing an online BOCES request form to add, modify or delete network user access and permissions. The IT Director receives paper requests from various staff members which he reviews prior to submitting the online form. BOCES, once it receives the request, uses configured specialized software to automatically manage the District's network 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.

We examined all 4,721 enabled network user accounts (3,745 student accounts, 893 nonstudent accounts and 83 generic accounts) to determine whether accounts were necessary and appropriate. We found that generally network user accounts and permissions were adequately managed through an informal process by the IT Director in conjunction with BOCES. In addition, network security configurations were appropriately configured.

Semi-annually, BOCES provides a list of inactive network user accounts to the IT Director for his review. Although the IT Director stated he reviewed these lists as well as a list of employees from the District's human resource office three times a year, we found the District had unneeded, unused and shared network user accounts that were not disabled.

The IT Director stated that with over 1,000 employees and a manual system for adding or removing users accounts or modifying their permissions, some fell through the cracks. However, he is working to develop a digital system similar to BOCES that will minimize these occurrences. Further, the IT Director has configured security settings to limit user permissions to only those needed for their respective job duties.

Unneeded Network User Accounts – We found 181 inactive user accounts (11 student and 170 staff accounts) that were not used in the last six months. District officials reviewed these accounts and other similar accounts upon our request.

The IT Director said all the inactive student accounts were needed as well as 35 inactive network staff accounts that were for bus drivers and food service workers who do not generally access the network. Although the IT Director told us that the remaining 135 inactive network staff accounts were unneeded, only 106 were disabled along with 15 additional network staff accounts during audit fieldwork. However, five of the remaining 29 enabled inactive network staff accounts are for former employees. These accounts should have been disabled when the individuals separated employment. Because the accounts remained enabled, they are potential access points for cybercriminals to exploit.

Unneeded Generic User Accounts – We found 49 of the 83 generic user accounts were not used in the last six months. Officials reviewed these accounts and disabled three unnecessary generic accounts. The IT Director told us that he would conduct a more in-depth review of 27 of the remaining 46 inactive generic user accounts to determine if they will be needed for the upcoming instructional year. He further stated that they are most likely unneeded and will be disabled in September 2021 once he has completed a more in-depth review.

In total, officials disabled 124 network user accounts and may disable up to another 27. Unneeded network user accounts can be potential entry points for attackers because they are not monitored or used and, if accessed by an attacker, could be used to inappropriately access and view PPSI. Also, when the District has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access. In addition, if users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Why Should the District Have an SLA With its IT Service Provider?

District officials must ensure they have qualified IT personnel to manage and secure the district's IT environment. This can be accomplished by using district employees, an IT service provider or both. To protect the district's network and avoid potential misunderstandings, officials should have a written SLA with the district's IT service provider that clearly identifies the district's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI.

An SLA is different from a traditional written contract in that it establishes comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement, scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The SLA should be reviewed by knowledgeable IT staff, legal counsel, or both, and be periodically reviewed, especially if the IT environment or needs change significantly.

Unneeded network user accounts can be potential entry points for attackers…to inappropriately access and view PPSI.

District Officials Did Not Have an SLA With BOCES

District officials engage BOCES to provide various IT support and services such as network management, IT support and management, Internet filtering, backups and firewall/intrusion detection by selecting certain items from a list of available services. The cost of the services for the 2019-20 fiscal year totaled more than $2.14 million. Although officials paid BOCES more than $2 million for IT services for the 2019-20 fiscal year, officials did not have a formal agreement or SLA with BOCES to identify the responsibilities and specific services BOCES was paid to provide.

While officials chose BOCES IT products and services by selecting certain items from a list of available IT services, the list did not provide detailed explanations of the services or their associated costs. As a result, officials were unable to determine exactly what services they paid for and whether they were appropriately billed. In addition, officials cannot determine if they were receiving the best value for similar goods and services offered by other IT service providers.

Further, officials had no procedures in place to monitor and review the work performed by BOCES staff or ensure the District's IT assets and data were safeguarded.

Why Should the District 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 and communicates related policies and procedures to all employees and students. 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. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

District Employees Were Not Provided With IT Security Awareness Training

The District did not provide users with IT security awareness training to help ensure they understood IT security measures. Instead, the IT Director provided information through emails about potential security threats they should be aware of.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. 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, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

The Board should:

1. Adopt policies and procedures for managing user accounts, including adding, disabling and changing user permissions.
2. Develop policies and procedures to monitor and review the work performed by BOCES staff to ensure the District's IT assets and data are safeguarded.
3. Develop an SLA with BOCES to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties, measurable performance targets and the related costs.

The IT Director should:

4. Regularly review and update network user accounts for necessity and appropriateness.
5. Routinely evaluate generic user accounts and disable those that are no longer needed.
6. Provide periodic IT security awareness training that reflects current risks to personnel who use IT resources.

Appendix A: Response From District Officials

Horseheads Central School District

Business Office
143 Hibbard Road • Horseheads, NY 14845
(607) 739-5601, x4260 • Fax (607) 795-2415
www.horseheadsdistrict.com

September 29, 2021

Edward V. Grant Jr., Chief Examiner
The Powers Building
16 West Main Street- Suite 522
Rochester, New York 14614-1608

Re: Horseheads Central School Network Access Controls Report of Examination 2021M-127

Dear Mr. Grant:

The Horseheads Central School District (District) is in receipt of the draft Network Access Controls Report of Examination 2021M-127 for the period of July 1, 2019 – August 11, 2021. On behalf of the Board of Education, Superintendent, and District administration, we appreciate the opportunity to respond to the findings of this report.
First, we would like to thank the auditors for their professionalism and consideration during this very thorough and in-depth audit of the District's network access. Secondly, we are pleased to note that this examination did not identify any areas of fraud within the Horseheads Central School District.
The District appreciates the feedback in this report, as we continuously strive to improve all our processes and procedures. We have a dedicated technology team who works very hard to maintain network security. We enjoyed our conversation with the auditing team during the exit conference and appreciated the fact they said our work in the district is commendable regarding our network security. We are thankful for the compliment and will use the feedback in this report for the betterment of the district.
In response to the findings of this report:

1. *Officials Did Not Adopt Formal Policies and Procedures to Manage Network User Accounts and Permissions*

The District acknowledges that it does not have formal written policies and procedures. However, it should be noted that the District is not lacking in procedures. The District would also like to note that out of the total 4,721 enabled accounts (student, staff, and generic), only 230, or 4.8%, were noted by this audit. The removal of old accounts has been something that the District's technology department was actively working on prior to and during this audit and we appreciate the additional assistance of the auditing team in helping identify those that required deleting.
The District has informal procedures that we continue to make improvements upon. The current Director of Technology has streamlined former practices of informal email/phone call communications from supervisors and clerical staff for the account set up of new hires, removal of separations, and updates of position changes. The Director of Technology has created a standardized electronic form, completed by a supervisor, that adds, modifies, or deletes an employee's access. Once submitted, this form goes to the Human Resources department, the Director of Technology, and the department's clerical support:

- Human Resources confirms that the new hires have met all hiring requirements, including fingerprint clearance, to continue the new employees' set up.
- After Human Resources approval, the Director of Technology or the clerical support makes a request to GST BOCES to set up the employee with the appropriate system access. All retirements/resignations/terminations will have access removed upon separation.
- The Director of Technology and the clerical support also review the monthly board of education approved Human Resources recommendations to confirm all separations are accounted for and access removed accordingly.
- As another layer of review, the Director of Technology and the clerical support also periodically review an active directory report provided by GST BOCES that contains information regarding users' accounts including number of log-ins, date the account was created, last log-in by the user, the last wrong password attempt on that account,

of log-ins, date the account was created, last log-in by the user, the last wrong password attempt on that account, the number of wrong password attempts, and if the user's password had expired. The Director of Technology and team of local area network technicians will review the active directory report and identify users that appear to be inactive or not accessing their account over a 60-day period. The Director of Technology will confirm with supervisors if there is a question regarding the employment status of someone on the report and make access adjustments accordingly.

Student accounts are handled in a manner different from employees. Student accounts are automatically created when a student is registered in our district. If a student unenrolls (graduates, homeschool, etc.), there is an automated process that purges the student from the system. An "inactive" student account occurs when there is a delay between an account being set up and the student actually starting. For example: The District is notified of a new student enrolling in the district on September 30 with an effective date of December 1. The account is created prior to the student's arrival and will show inactive until the December 1 start. Therefore, the eleven inactive student accounts noted in this report were in a transitional phase and needed to stay in the system.

See Note 1 Page 9

Generic accounts, defined as accounts not assigned to a specific person, will continue to be reviewed and removed as they become unnecessary. Many have been deleted to date. All generic accounts are reviewed and approved by the Director of Technology. Examples of generic accounts that have been deemed necessary are internal accounts such as Instructional Support and Horseheads Technology Services, and external accounts such as our provider of network controls in order for them to have access to functionality and maintenance.

2. *District Officials Did Not Have an SLA With BOCES*

The District acknowledges the concept of a service level agreement with GST BOCES to identify the responsibilities and specific services GST BOCES is paid to provide. The District has a long, successful history with GST BOCES with the various IT support and services they provide. The District will share this recommendation with GST BOCES as this is something the GST BOCES administration would need to create and disseminate amongst all component districts. This is not a document or process any district would initiate as a stand-alone agreement with GST BOCES.

See Note 2 Page 9

3. *District Employees Were Not Provided with IT Security Awareness Training*

The Districts acknowledges that it currently does not provide formal IT security awareness training for all district staff. However, the District does have informal means of communicating such information. As situations arise, the Director of Technology will email all staff regarding IT security matters they need to be aware of. New this year, the District has incorporated IT security awareness training by our Director of Technology into our new hire orientation. The District has also obtained IT security awareness training modules from GST BOCES that we are currently vetting for use. In addition, we are working with our cyber insurance carrier for training opportunities. IT security awareness training will be given to our staff prior to the end of this calendar year, and incorporated into our annual trainings, like our Right to Know training.

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

Very Truly Yours,

Kristine Dale
President, Board of Education

Dr. Thomas J. Douglas
Superintendent of Schools

Appendix B: OSC Comments on the District's Response

Note 1

This explanation significantly differs from that provided during the audit where an official identified the 11 inactive students as either Pre-K students using an iPad or special education students.

Note 2

Both parties should be involved in defining the terms and understand the services to be provided, especially when BOCES uses third-party vendors for some of those services. Developing a good SLA can help avoid costly misunderstandings and establish an efficient, secure computing environment.

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 reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of IT operations, specifically those related to the granting, modification and revocation of network user accounts and permissions.
- We examined network user account and security settings using specialized audit scripts. We reviewed the network user and administrator accounts and compared them to current employee lists to identify inactive and possibly unneeded network user 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 IT controls.

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

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

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