REPORT OF EXAMINATION | 2021M-108

Haverstraw-Stony Point Central School District

Information Technology

DECEMBER 2021

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

Contents

Report Highlights

Haverstraw-Stony Point Central School District

Audit Objective

Determine whether Haverstraw-Stony Point Central School District (District) officials established adequate internal controls over user accounts to prevent unauthorized use, access and loss.

Key Findings

Officials did not establish adequate controls over the District's user accounts to protect against unauthorized use, access and loss. Officials did not:

- Establish written procedures for granting, changing or disabling network user accounts or user permissions.
- Disable 130 unneeded generic and nonemployee network user accounts of the 475 network user accounts examined.
- Provide information technology (IT) security awareness training to all employees using IT resources.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop and implement written procedures for granting, changing and disabling user access.
- Provide periodic IT security awareness training to all employees who use IT resources.

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

Background

The District serves the Towns of Haverstraw and Stony Point in Rockland County. The District is governed by a Board of Education (Board), which has seven elected members.

The Superintendent of Schools (Superintendent) is appointed by the Board and is the chief executive officer responsible for day-to-day management, under the Board's direction.

The District's Director of Technology (Director) is responsible for monitoring network user accounts.

Quick Facts	
Students	7,843
Employees	1,238
Network User Accounts	
Student	8,680
Employee	1,092
Non-employee	275
Generic	200
Total	10,247

Audit Period

July 1, 2019 – December 21, 2020. We extended our audit period forward through March 8, 2021 to complete our IT testing.

Information Technology

The District's IT system and data are valuable resources. The District relies on its IT assets for Internet access, email and maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI).[1] If the IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

... [D]istrict officials should regularly review enabled network user accounts... and disable unnecessary accounts. ...

How Should District Officials Manage Network User Accounts?

Network user accounts provide access to network resources and should be actively managed to minimize the risk of misuse. 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. A district should have written procedures for granting, changing and disabling user permissions. In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed. Officials should disable unnecessary accounts as soon as there is no longer a need for them.

Generic accounts are not linked to individual users and may be needed for certain networks services or applications to run properly. 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 and disable any generic accounts that are not related to a specific system need.

Officials Did Not Adequately Manage Network User Accounts

The Director was responsible for ensuring network user accounts were managed in a timely and satisfactory manner. However, network user accounts were inadequately managed. Officials did not maintain a list of authorized network users. As a result, we found 130 unneeded network user accounts that had not been disabled.

Further, the District did not have written procedures for granting, changing and disabling user permissions. The Director maintained a schedule of when new employees were added, and users authorized by the Board to be removed. In addition, a list of all authorized users was available from the system. However, the Director did not review the system list (which can change daily) and some of

1 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.

the unneeded accounts were created before he was appointed. As a result, the Director did not properly review and monitor the access of all users.

We reviewed all 200 generic network user accounts and found 82 were no longer needed. These included past vendors and accounts for previously used software management. We also reviewed all 275 nonemployee network user accounts[2] and found 48 were no longer needed. The IT director said these were in place before he started. In addition, we identified 54 former employee accounts that had not been used in at least six months. The Director said they would further investigate the former employee accounts to determine whether they should be disabled.

The Director told us he is not notified when network accounts are no longer needed and that he disabled the 130 unneeded network user accounts we identified. However, the Director should periodically print a list of users from the system and verify whether all users are active and disable those that are no longer needed. Without written procedures, employees may not be aware of their responsibilities when staff leave District employment.

If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network or to gain access to or control over other IT functions. 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.

Why Should 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 to all employees. It is also important for district officials to take this training so they keep current on the evolving security threats and the policies and procedures that should be in place to reduce risk. The training should explain policies and procedures adopted by district officials and communicate the proper rules of behavior for using the Internet and IT systems and data.

The training should center on emerging trends such as information theft, social engineering attacks, 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, administrators or IT staff) and include everything that attendees need to perform their jobs.

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

2 Nonemployee accounts included those of Board members and third-party contractors. Most of the time generic accounts are assigned to software vendors and many are built-in user accounts.

The training should also 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.

District Officials Did Not Provide IT Security Awareness Training

District policy states the Director is responsible for providing in-service programs for the training and development of District staff in computer skills, and for incorporating computer use in appropriate subject areas. Further, the policy requires the District to provide annual training on data privacy and security awareness to all employees who have access to PPSI.

District officials did not provide all employees with IT security awareness training to help ensure they understand IT security measures designed to safeguard data and IT assets. We selected a sample of seven employees who regularly access PPSI and found that five office staff had not received IT security awareness training. In addition, the District did not maintain records of IT training attendance and could not ensure all employees received training.

The Director said the District annually provided faculty security awareness training. However, non-instructional staff, including Board members and other officials, were overlooked and not included in the training. As a result, IT assets and data were more vulnerable to loss and misuse. After we brought this to the attention of District officials, they told us they have scheduled cybersecurity training for all employees at the end of the current school year.

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 loss.

What Do We Recommend?

District officials should:

1. Routinely attend IT security awareness training to stay informed of evolving threats that should be addressed in policies and procedures.
2. Develop written procedures for granting, changing, and disabling user permissions.

The Director should:

3. Maintain a list of authorized users and routinely evaluate and disable any unnecessary accounts.

4. Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use and maintain training attendance records.

Appendix A: Response From District Officials

NORTH ROCKLAND
CENTRAL SCHOOL DISTRICT

KRIS F. FELICELLO, Ed.D.
Superintendent of Schools

ILEANA ECKERT ADMINISTRATIVE OFFICE BUILDING
65 Chapel Street, Garnerville, New York 10923 • (845) 942-3000

November 17, 2021

Lisa Reynolds Chief Examiner
Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive Suite 103
New Windsor, New York 12553

To Ms. Reynolds:

Please let the information below serve as the North Rockland Central School District's response to the recent technology audit. The areas in which the district was cited for improvement are addressed below with corrective actions included. The North Rockland Central School District is in agreement with the findings. In addition, we would like to thank the Office of the State Comptroller for the professional manner in which the audit was conducted. The findings from this audit will only help our district improve its information technology system.

Summary of Findings:

- Establish written procedures for granting, changing, or disabling network user accounts or user permissions
- Disable 130 unneeded generic and nonemployee network user accounts of the 475 network user accounts examined
- Provide information technology (IT) security awareness training to all employees using IT resources

Recommendations:

- Develop and implement written procedures for granting, changing, and disabling user access. District Agrees
- Provided periodic IT security awareness training to all employees who use IT resources. District Agrees

Corrective Action Plan:

1. Develop and implement written procedures for granting, changing, and disabling user access.
    a. The district has a small team of authorized staff members who have district approval to make any changes or additions to employee network accounts. When a new employee is hired by the district the Personnel Office initiates the creation of an by completing an electronic form which contains name, position, start/end date, and location. The authorized IT staff creates the user accounts and permissions according to the role the employee is being hired for. If there is an internal position change the same process is followed and permissions are

either granted or removed. This procedure is being updated and documented in the district's IT policies as of December 2021.

b. If a generic account is needed a Service Desk desk ticket is created and the generic account is sent to the Director of Information Systems for approval. All generic accounts will have a start and end date. This has been completed as of July 2021.

c. The IT Staff during the first 2 weeks of July annually will conduct an audit of Active Directory. This will ensure that all generic accounts are disabled. In addition an employee list from the district financial database will be used to review current employees and disable any accounts that will be disabled because of no longer being employed by the district.

2. The district will be training all staff members in IT security awareness on a periodic basis. Methods by which training will be conducted:

   a. [redacted] will be a training platform that will deliver training to all employees that use IT resources. Through [redacted] employees will take a course that will cover cyber awareness such as understanding cyber attacks, password security, data privacy, phishing emails, and social engineering. Training will start December 2021 and continue yearly.

   b. [redacted] will conduct phishing email campaigns on district employees. For employees that are phished additional training will be provided through the platform. This training is ongoing throughout the school year.

   c. The Director of Information Systems will also send out Cyber Awareness information to employees via email.

Sincerely,

Kris Felicello, 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 to gain an understanding of the District's user accounts and determine the adequacy of the policies and procedures.
- We interviewed District officials and reviewed records to gain an understanding of procedures related to monitoring and managing user accounts.
- We inquired with District officials and seven employees who had access to PPSI regarding whether they received IT security awareness training and how they are notified of policy changes and updates to the IT policy.
- We used our professional judgment to select a sample of seven District computers from the 32 computers of employees who had access to PPSI. Our sample included five business office computers, one computer guidance computer and one special education computer. We ran a computerized audit script on each of the seven selected computers to analyze reports generated by the script, to identify weaknesses in local user account security policies, settings and software.
- We ran a computerized audit script to examine the District domain controller.[3] We then analyzed the report by comparing user accounts to a list of current employees to determine whether any network users were no longer employed by the District.

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

3 The server that controls or manages access to network resources.

the value and/or size of the relevant population and the sample selected for examination.

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