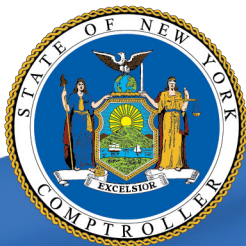


Peekskill City School District

Network User Accounts

JUNE 2022



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

Contents

Report Highlights 1

Network User Accounts 2

 How Should Officials Manage and Monitor Network User
 Accounts? 2

 District Officials Did Not Adequately Manage and Monitor
 Network User Accounts 2

 Why Should District Officials Provide IT Security Awareness
 Training? 4

 All IT Users Did Not Receive IT Security Awareness Training 4

 What Do We Recommend? 5

Appendix A – Response From District Officials 6

Appendix B – Audit Methodology and Standards 7

Appendix C – Resources and Services. 8

Report Highlights

Peekskill City School District

Audit Objective

Determine whether Peekskill City School District (District) officials adequately managed and monitored network user accounts.

Key Findings

District officials did not adequately manage and monitor network user accounts. In addition to sensitive information technology (IT) control weaknesses which we communicated confidentially to officials, we found District officials should have:

- Disabled 133 of the District's 821 network user accounts. These accounts consisted of 56 individual and 77 generic unneeded network user accounts, one of which was last logged on in January 2012.
- Ensured all users using IT resources received periodic IT awareness training.

Key Recommendations

- Periodically review enabled network user accounts and ensure that unneeded user accounts are immediately disabled.
- Provide periodic IT security awareness training to all users who use IT resources.

District officials agreed with our recommendations and indicated they will take corrective action.

Background

The District is located in the City of Peekskill in Westchester County.

The District is governed by an elected seven-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's Manager of Educational Technology (IT Manager) is responsible for managing the District IT assets including network security and user accounts. The District contracts for onsite information technology services to support the IT Manager in her duties.

Quick Facts

Non-Student Network User Accounts

Staff	576
Generic	156
Non-Employee	89
Total	821
Onsite IT Contractors Third Party Expense	\$583,619

Audit Period

July 1, 2019 – June 11, 2021.

Network User Accounts

Network user accounts provide access to network resources and should be actively managed and monitored to minimize the risk of misuse. Generic accounts are not linked to individual users and may be needed for certain networks services or applications to run properly. If network user accounts are not properly managed and monitored, 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 on the network.

How Should Officials Manage and Monitor Network User Accounts?

To minimize the risk of unauthorized access, officials should disable unnecessary accounts as soon as there is no longer a need for them. In addition, to minimize the risk of unauthorized access, school district officials should maintain a list of authorized user accounts and regularly review enabled network user accounts to ensure they are still needed.

Generic accounts are not linked to individual users and may be needed for certain network 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 generic network user accounts and disable those that are not related to a current district or system need. Additionally, each user should have his or her own user account to ensure accountability. When multiple users are allowed to share user accounts, activity in the system may not be able to be trace back to a single user.

District Officials Did Not Adequately Manage and Monitor Network User Accounts

District officials did not adequately manage and monitor network user accounts. After their most recent review of user accounts in May 2021, they did not follow up with Human Resources to determine why they did not receive notification that accounts needed to be deleted and did not disable or delete the accounts until they determined whether or not the accounts were still essential.

Unneeded Generic Accounts

We reviewed all 156 generic accounts and inquired with the IT Manager whether these accounts were needed. We found 77 unneeded generic network user accounts, one of which was last logged on in January 2012. The IT Manager stated that although they do have an informal procedure in place to delete

...[O]fficials
should
disable
unnecessary
accounts as
soon as there
is no longer
a need for
them.

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 (students), third parties or other individuals or entities.

unneded accounts, it was not always followed. When they last reviewed the network user accounts in May 2021, she stated that, unfortunately, they had missed some accounts. She said they were working with human resources to determine why they were not notified to delete the accounts. The remaining 79 generic accounts are needed to run certain programs and services, and some are used by technicians for test settings.

Because generic accounts are shared accounts, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user.

Unneeded Non-Student Accounts

We compared the remaining 665 non-student user accounts (i.e., not generic) to the employee master list and found there were 56 unneeded network user accounts that were still enabled on the network. These accounts were removed when we brought this to the IT Manager's attention.

Unneeded network user accounts are entry points for attackers, as they could be used to inappropriately access and view PPSI. Also, when a district has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access. When network user accounts are not used or monitored, compromised accounts may not be detected timely.

While the District does not have written procedures for managing network users accounts, they do have a process for removing unneeded user accounts. The IT Manager told us that when an employee is hired or terminated, the Human Resources department sends the Technology Department a personnel change form requesting they grant, modify or disable the employee's network user account. These forms alert the Technology Department of a new or terminated employee. When an employee is terminated, their procedure is to disable the account for 30 days and then delete it. These accounts are not deleted immediately because often these employees return as consultants, or the technicians are asked to locate specific files or emails. For generic and non-student network accounts the IT Manager would provide a list of network user account names enabled on the network to Human Resource annually to verify which accounts are still needed and then the IT Manager would have the unneeded accounts removed. This procedure was last done in May 2021. However, there were 133 unneeded generic and other non-student network user accounts that went unaddressed until our audit. In addition, she did not maintain a list of authorized users or regularly review enabled network user accounts to ensure they were still needed.

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, 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, 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 email, Internet browsing, downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

All IT Users Did Not Receive IT Security Awareness Training

District officials did not ensure all users received periodic IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets. Although the IT Manager and the Operations Manager received cyber security training during our audit period, no other employees have received training.

The IT Manager told us that the District had to divert the funds that were dedicated for cyber security training to use during the pandemic. However, Human Resources is in the process of incorporating cyber security awareness training as part of the mandatory trainings required by all employees. The IT Manager also shared the names of two companies that she has contacted to provide training to the District. At the end of our field work, the District hired one of the two consulting companies and began training for all employees. The IT Director told us that a monthly phishing video will be sent to all employees and training will include topics such as phishing, malware, safe web browsing and social engineering.

Without periodic comprehensive 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.

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

What Do We Recommend?

The District IT Manager should:

1. Develop written procedures for granting, changing and disabling network user account access and monitor to ensure procedures are being followed.
2. Disable network user accounts of former employees as soon as they leave District employment, periodically review existing network user accounts, including generic and any non–student accounts and disable any deemed unneeded.
3. Provide periodic comprehensive IT security awareness training that includes guidance on the importance of appropriate computer use to all users who use IT resources.

Appendix A: Response From District Officials



Peekskill City School District

Our mission is to educate and empower all students to strive for excellence as life-long learners who embrace diversity and are contributing members of a global society.

Dr. David Mauricio

Superintendent of Schools

Administration Center, 1031 Elm Street, Peekskill, NY 10566-3499

Phone: (914)737-3300 ext. 1531 Fax: (914) 737-3722

Email: dmauricio@peekskillschools.org

May 3, 2022

STATE OF NEW YORK OFFICE OF THE STATE COMPTROLLER

Newburgh Regional Office

33 Airport Center Drive

Suite 103


New Windsor, NY 12553

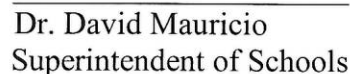
To whom it may concern:

The Peekskill School District is in receipt of the draft Report of Examination regarding its Network User Accounts for the audit period July 1, 2019 to June 11, 2021. Please accept this letter as the District's response to the Draft Report. We acknowledge the findings and recommendations set forth in the draft Report. The Board of Education and Central Office Administration view such findings and recommendations as an opportunity to continue their ongoing efforts to implement policies and procedures that provide users, employees, and the school community with a safe, sound, and beneficial educational IT environment in the District.

The District would like to take this opportunity to thank the representatives of the Office of the Comptroller for their hard work and professionalism throughout this comprehensive process, along with their insight and assistance.

Sincerely,


Ms. Jillian Villon
BOE President


Dr. David Mauricio
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, employees and the third-party contractor and reviewed the District's IT-related policies to gain an understanding of the IT environment, internal controls and training. Further, we met with the IT Manager to determine if any accounts were no longer needed and if so, to gain an understanding of why the accounts remained on the network.
- We ran a computerized audit script on the District's network on June 11, 2021 to examine the District's domain controller. We then analyzed the report by comparing network user accounts to a list of current employees to identify former employees and/or unneeded accounts, reviewed for weaknesses in user account management and network setting configuration.

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.

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 – Dara Disko-McCagg, 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: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties



Like us on Facebook at facebook.com/nyscomptroller

Follow us on Twitter [@nyscomptroller](https://twitter.com/nyscomptroller)