REPORT OF EXAMINATION | 2021M-142

New Rochelle City School District

Information Technology

DECEMBER 2021

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

Contents

Report Highlights

New Rochelle City School District

Audit Objective

Determine whether New Rochelle City School District (District) officials established adequate controls over network and financial application user accounts to prevent unauthorized access, use and/or loss.

Key Findings

Officials did not establish adequate controls over network and financial application user accounts to prevent unauthorized use, access and/or loss. In addition to sensitive information technology (IT) control weaknesses which we communicated confidentially to officials, we found officials did not:

- Adequately manage network user accounts.
  - 84 former employees/vendors had active user accounts.
  - 35 generic user accounts that had never been used and were unnecessary.
- Ensure District procedures were followed to communicate financial application user account changes to the vendor.

Key Recommendations

- Develop written procedures for managing network access that include periodically reviewing user access and disabling network user accounts when access is no longer needed.
- Evaluate all existing financial application user accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.

District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The District is located in the City of New Rochelle, in Westchester County. The District is governed by an elected nine-member Board of Education (Board). The 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 contracts with an IT vendor to operate and maintain the District's IT system. The District's IT Director is responsible for overseeing and implementing IT controls as directed by the Board and Superintendent. The Assistant Superintendent for Business (Assistant Superintendent) works with the IT vendor to manage the District's financial application.

Quick Facts	
Students	10,164
Employees	2,229
Network User Accounts	
Generic	97
Non-Student	1,519
Student	10,164
Reviewed (Generic and Non-Student)	1,616

Audit Period

July 1, 2019 – April 30, 2021. We extended our scope forward to May 4, 2021 to complete 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 personnel records that contain personal, private and sensitive information (PPSI).[1] The system also includes the District's financial software, which contains extensive PPSI about employees including Social Security numbers, medical information, retirement registration numbers and bank account numbers.

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.

How Should Officials Manage User Accounts?

User accounts provide access to the network and the financial application 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 the network and view PPSI on the network and in the financial application. Therefore, a district should have a written policy and procedures for granting, changing and revoking access rights to the network and financial application.

In addition, to minimize the risk of unauthorized access, district officials should maintain a list of authorized user accounts and regularly review enabled user accounts to ensure they are still needed. Officials should disable unnecessary accounts as soon as there is no longer a need for them, including user accounts of former employees or employees who have left the district or transferred to another area. This helps ensure PPSI is protected from unauthorized access.

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 and disable any generic accounts that are not related to a specific need.

Officials Did Not Adequately Manage User Accounts

Officials did not adequately manage network and financial application user accounts, which increases the risk of unauthorized access, use and/or loss.

---

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.

We reviewed all 1,616 non-student network user accounts, which includes 151 financial software user accounts.

Network User Accounts – Of the 1,616 non-student network user accounts, we identified 84 network user accounts that were for former employees or third-party contractors who no longer worked at the District. Some of these users left District service over four years ago. In addition, of the 97 active generic user accounts we found another 35 unneeded network user accounts that were originally created for various uses but had never been used and should be disabled. For example, some of these unneeded users were created in 2019 and never used.

The District did not have procedures for granting, changing or disabling network user accounts. Furthermore, because officials did not maintain a current list of authorized users, it was significantly more difficult given the number of users on the system to review or monitor user access. When we informed District officials of the unnecessary user accounts, they agreed to disable unnecessary network accounts immediately.

If unneeded network user accounts are accessed by an attacker, the entry point could be used to inappropriately access and view PPSI without detection. Also, having many unneeded user accounts makes it more difficult to adequately manage network access.

Financial Application User Accounts – We found that 23 of the 151 enabled financial application user accounts were assigned to former employees, some who have left employment at the District 47 months ago. Although the District has a process to communicate changes to employee status, District officials did not always provide a written directive to the IT vendor, per the District's process, to disable user accounts that are no longer needed. As a result, employees who were no longer employed by the District had active accounts within the application. We also found two enabled user accounts that District officials could not recall their purpose. These user accounts were assigned to former vendors.

We verified that the Assistant Superintendent disabled the 25 inactive user accounts after we brought them to his attention. The Assistant Superintendent stated that these users could only access the application when physically on-site or with permissions to access it through a Virtual Private Network (VPN). The Assistant Superintendent also stated that the District attempts to disable the user accounts for terminated employees in a timely manner. He also strives to keep communication lines open to ensure human resources identifies those individuals no longer employed by the District and to ensure that the IT vendor is notified timely of staff members who no longer need access to have their accounts deactivated.

Although these users would need to be on the District's network to access the application, the remaining risk level is still not acceptable. When inactive or

…[W]e idenified 84 network user accounts that were for former employees or third-party contractors who no longer worked at the District.

We found that 23 of the 151 enabled financial application user accounts were assigned to former employees....

terminated employees still have access to the District's financial application software, there is always an increased risk that intentional or unintentional changes could occur without detection or a greater risk that these accounts could be used as entry points for attackers to access personal information and compromise IT resources.

What Do We Recommend?

The IT Director should:

1. Develop written procedures for managing network access that include periodically reviewing user access and disabling network user accounts timely when access is no longer needed.
2. Maintain a list of authorized network users and routinely evaluate and disable any unnecessary accounts.
3. Inform the IT vendor when financial application users should be disabled.

The Assistant Superintendent should:

4. Develop written procedures for managing financial application access that include periodically reviewing user access and disabling financial application user accounts timely when access is no longer needed.
5. Maintain a list of authorized financial application users and routinely evaluate and disable any unnecessary accounts.
6. Inform the IT vendor when financial application users should be disabled.

Appendix A: Response From District Officials

CITY SCHOOL DISTRICT OF NEW ROCHELLE
515 NORTH AVENUE
NEW ROCHELLE, NEW YORK 10801-3416

JONATHAN P. RAYMOND
SUPERINTENDENT OF SCHOOLS

TELEPHONE: (914) 576-4200
FAX: (914) 632-4144
E-MAIL: JRAYMOND@NREDLEARN.ORG

December 2, 2021

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

RE: New Rochelle City School District
District Response to Information Technology – Report of Examination, 2021M-142
Audit Period July 1, 2019 – April 30, 2021 (extended to May 4, 2021)

Dear Ms. Reynolds,

It was a pleasure speaking with your staff on November 10, 2021 and we appreciate their review and explanation of the findings in the recent examination. The District agrees with those findings. In addition, thank you and your staff for taking the time to examine the District's Information Technology (IT) system. Your expertise and experience help to enhance our IT operations and the security of the data contained in that system.

We appreciate the efforts and work you do on behalf of our students and residents. Again, we thank you for the time you devoted to this report. Please note that the District has already addressed and implemented some of the recommendations in the report and will be providing the Board of Education a Corrective Action Plan (CAP) at an upcoming meeting. The CAP and copy of the resolution will be sent once it is approved. Please contact me if you have any questions or concerns.

Very truly yours,

Jonathan P. Raymond
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 network and financial application user accounts and determine the adequacy of the policies and procedures.
- We observed District officials generate reports with network configuration and user data from the District's domain controller.[2] We analyzed the data from these reports to identify weaknesses in user account management, privilege and group definitions and network setting configurations.
- We reviewed user access rights for the District's financial application to determine whether user accounts were needed and if access was properly assigned.

Our audit also examined the adequacy of certain IT 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.

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

2 A domain controller is a server that runs a database of centrally managed objects such as user and computer accounts along with their respective attributes. This database provides a centralized point of network authentication and security settings management.

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