DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-209

Port Chester-Rye Union Free School District

Information Technology User Accounts

JUNE 2022

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

Contents

Report Highlights

Port Chester-Rye Union Free School District

Audit Objective

Determine whether Port Chester-Rye Union Free School District (District) officials adequately managed non-student network user accounts to ensure unnecessary accounts were disabled.

Key Findings

District officials did not adequately manage non-student network user accounts to ensure unnecessary accounts were disabled. Specifically:

- District officials did not establish comprehensive written procedures to periodically review all network user accounts, identify unnecessary network user accounts and notify the IT vendor to disable them.
- Nine former employees' user accounts and 120 unneeded generic user accounts were not disabled on the network.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Maintain and periodically evaluate a list of authorized network user accounts and notify the IT vendor using service requests to disable network user accounts of former employees and other users that are no longer needed.

District officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comment on an issue raised in the District's response.

Background

The District is located in Westchester County. The District is governed by an elected five-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 has a Service Level Agreement (SLA) with an IT vendor to operate and maintain the District's IT system. The Deputy Superintendent of Schools (Deputy Superintendent) oversees the District's IT functions and controls at the direction of the Board. The Senior Facilitator/Educational Technology (Facilitator of Technology) reports to the Deputy Superintendent and manages the District's day-to-day IT operations.

Quick Facts	
2021-2022 IT Vendor Contract Amount	$615,549
Employees (Full and Part-time)	751
Students	4,775
Network User Accounts	
Student	6,469
Non-Student	829
Generic	237
Total	7,535
Reviewed Non-Student	829
Reviewed Generic	237
Total	1,066

Audit Period

July 1, 2019 – December 17, 2020. We expanded our audit period back to July 1, 2016 and forward through August 31, 2021 to review service requests and complete IT testing.

Information Technology

The District relies on its IT assets for maintenance of financial and personnel records, much of which contain personal, private and sensitive information (PPSI)[1], as well as email and Internet access. If the IT system is compromised, the results could be catastrophic and require extensive effort and resources to evaluate and repair or rebuild. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

How Should Officials Manage Network User Accounts?

Network user accounts provide access to the resources on a district's network (e.g., shared folders and email) 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 PPSI on the network. A district should have written procedures for granting, changing and revoking access rights to the network. In addition, to minimize the risk of unauthorized access, officials should regularly review enabled network user accounts to ensure they are still needed and ensure unnecessary user accounts are disabled as soon as they are no longer needed. The ability to create or modify network user account access should be limited to authorized personnel.

The use of generic network user accounts should be limited. 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 purposes, 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.

Officials Did Not Adequately Manage Network User Accounts

Officials did not properly manage network user accounts or maintain a current list of authorized users and their level of access. District officials did not perform periodic reviews of all District network user accounts to identify any unnecessary network user accounts. According to the Facilitator of Technology, as of July 2021,

[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 individual or entities.

no review of network user accounts had been performed within the last year to year and a half. We examined the 1,066 non-student and generic network user accounts to determine whether any were unneeded and found:

- 220 network user accounts that did not match the District's employment records. We reviewed 25 of the 220 user accounts and found nine were for former District employees that were not disabled on the network. For example, the user accounts of a special education director who retired in July 2016, a custodian who retired in September 2018, and an administrative employee at the high school who retired in December 2020 were not disabled on the network.
- 173 of the 237 generic network user accounts on the network were never used to log onto the network. The Facilitator of Technology indicated that 120 were for substitute teachers and were no longer needed. Further, for an additional 90 generic user accounts, District officials provided no explanation as to whether the accounts were necessary. After informing the Facilitator of Technology about the generic accounts, she told us that the unneeded generic user accounts were subsequently disabled.

We attribute these findings, in part, to the officials not developing policies and procedures for managing network user accounts. According to the SLA, District officials are responsible for notifying the IT vendor to disable network user accounts through the creation and submission of a service request. While the IT department had an exit checklist that outlined the initial steps for deactivating network user accounts for employees separating from the District, we found that District officials did not always submit service requests to the IT vendor to disable network user accounts that were no longer needed.

According to the Facilitator of Technology, the IT department may not have notified the IT vendor to disable accounts due to a decentralized process where computer aides for each school building were responsible for notifying the IT vendor to disable network user accounts. Despite this, a periodic review of all network user accounts would have detected any unnecessary network user accounts that were not disabled.

Leaving former employee and unneeded generic user accounts on the network increases the risk of unauthorized access because any account on a network is a potential entry point for attackers. Of particular risk are network user accounts for former employees, as these could potentially be used by those individuals for malicious activities

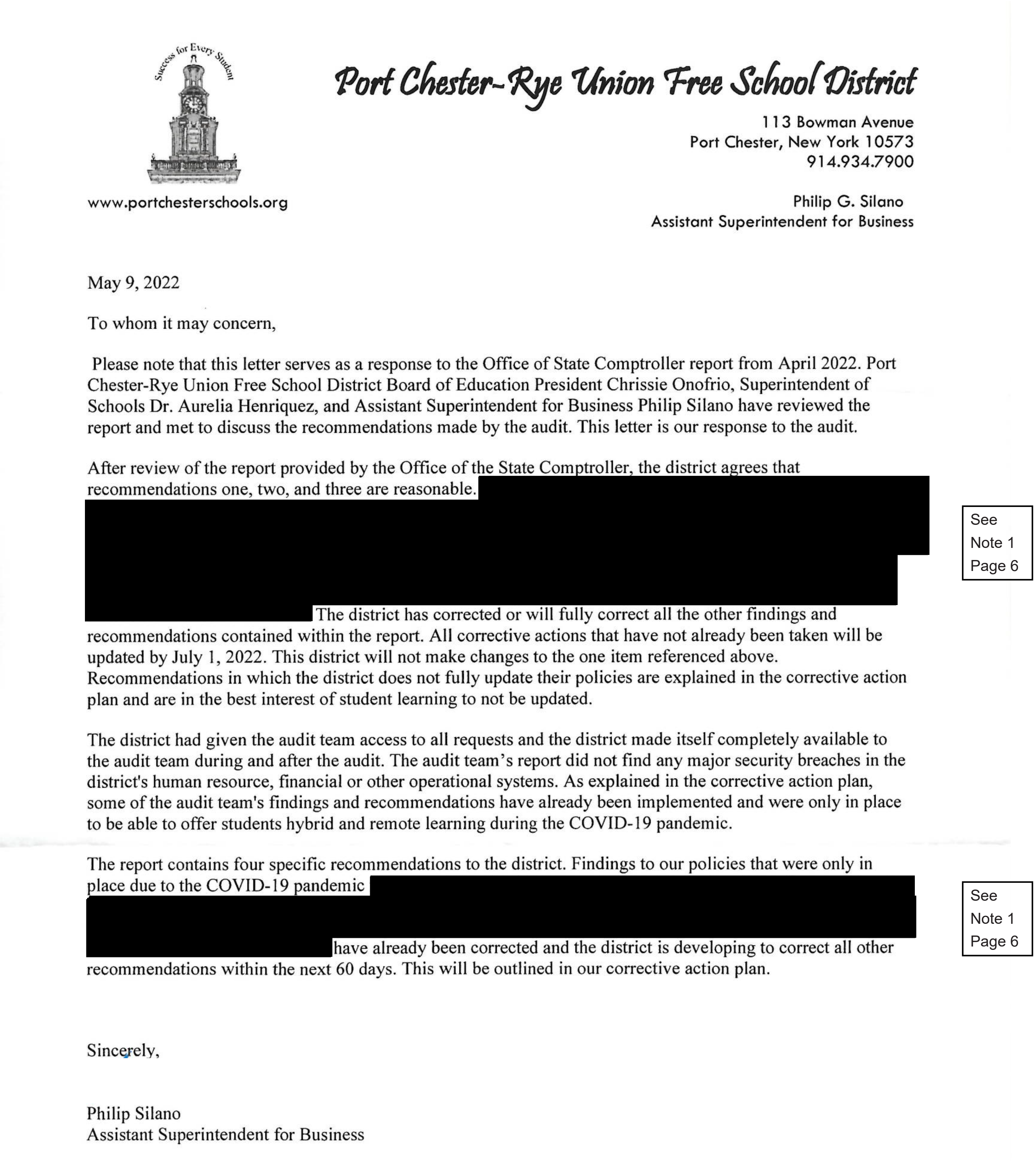
What Do We Recommend?

District officials should:

1. Establish formal written procedures for managing network user accounts and notifying the IT vendor using service requests to disable the accounts.

2. Maintain and periodically evaluate a list of authorized network user accounts and notify the IT vendor using service requests to disable network user accounts of former employees and other users that are no longer needed.

Appendix A: Response From District Officials



Success for Every Student

Port Chester-Rye Union Free School District

113 Bowman Avenue
Port Chester, New York 10573
914.934.7900

www.portchesterschools.org

Philip G. Silano
Assistant Superintendent for Business

May 9, 2022

To whom it may concern,

Please note that this letter serves as a response to the Office of State Comptroller report from April 2022. Port Chester-Rye Union Free School District Board of Education President Chrissie Onofrio, Superintendent of Schools Dr. Aurelia Henriquez, and Assistant Superintendent for Business Philip Silano have reviewed the report and met to discuss the recommendations made by the audit. This letter is our response to the audit.

After review of the report provided by the Office of the State Comptroller, the district agrees that recommendations one, two, and three are reasonable. [redacted] The district has corrected or will fully correct all the other findings and recommendations contained within the report. All corrective actions that have not already been taken will be updated by July 1, 2022. This district will not make changes to the one item referenced above. Recommendations in which the district does not fully update their policies are explained in the corrective action plan and are in the best interest of student learning to not be updated.

See Note 1 Page 6

The district had given the audit team access to all requests and the district made itself completely available to the audit team during and after the audit. The audit team's report did not find any major security breaches in the district's human resource, financial or other operational systems. As explained in the corrective action plan, some of the audit team's findings and recommendations have already been implemented and were only in place to be able to offer students hybrid and remote learning during the COVID-19 pandemic.

The report contains four specific recommendations to the district. Findings to our policies that were only in place due to the COVID-19 pandemic [redacted] have already been corrected and the district is developing to correct all other recommendations within the next 60 days. This will be outlined in our corrective action plan.

See Note 1 Page 6

Sincerely,

Philip Silano
Assistant Superintendent for Business

Appendix B: OSC Comment on the District's Response

Note 1

The portions of the response that commented on the confidential IT letter were redacted.

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 interviewed District officials, employees and contracted employees and reviewed IT policies and procedures to gain an understanding of the District's IT environment and determine the adequacy of internal controls over network and local user accounts.
- We reviewed the District's SLA with the IT vendor to gain an understanding of the services provided.
- On February 4, 2021, we ran a computerized audit script on the District's domain controller, which is the main server computer in the domain (network) that controls or manages all computers within the domain. We analyzed the data produced to assess network user accounts, permissions assigned to the accounts and the related security settings applied to the accounts.
- We compared the 829 non-student network user accounts to the active employee list to identify accounts for former employees and/or other accounts that may be unneeded. We also judgmentally selected 25 of the 220 network user accounts not on the District's employee list based on last login and user permissions and asked the Facilitator of Technology whether the network user account was needed and to provide a valid reason for needed network user accounts.
- We reviewed all 237 generic network user accounts and asked the Facilitator of Technology whether each generic network user account was needed and to provide a valid reason for the needed network user accounts.

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 GAGAS (generally accepted government auditing standards). 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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

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

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