DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-107

Chester Union Free School District

Information Technology

MARCH 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Chester Union Free School District

Audit Objective

Determine whether Chester Union Free School District (District) officials adequately managed and monitored network user accounts.

Key Findings

District officials did not adequately manage and monitor network user accounts. District officials should have:

- Disabled unneeded network user accounts when there was no longer a need for them.
- Monitored network user compliance with the District's computer acceptable use policy (AUP) by reviewing computer website history logs for appropriateness.

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

Key Recommendations

- Routinely evaluate and disable any unneeded network user accounts.
- Monitor Internet use to ensure network users comply with the AUP.

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

Background

The District is located in the Town of Chester. It serves portions of the Towns of Chester, Goshen and Blooming Grove and the Village of Chester in Orange County.

The District is governed by a Board of Education (Board), which includes five elected members.

The Superintendent of Schools (Superintendent) is appointed by the Board and is responsible for the District's day-to-day management.

The District's Data Administrator IT Director (IT Director) is responsible for all District IT functions and manages all IT infrastructure.

Quick Facts

Network User Accounts Reviewed	
Employee Accounts	159
Nonemployee Accounts	17
Generic Accounts	26

Audit Period

July 1, 2019 – January 11, 2021. We extended our audit scope through March 18, 2021 to complete our IT testing.

Information Technology

The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records. If its IT assets are compromised, the results could range from inconvenience to significant damage and could require extensive effort and resources to evaluate and repair.

While effective controls will not guarantee the safety of the District's computer system, without them the District has a significantly increased risk that its data, hardware and software systems could be lost or damaged by inappropriate access and use. Effective controls include managing and monitoring network user accounts to ensure users are appropriately accessing the Internet, emails, financial applications and personnel and student records.

How Should District Officials Manage Network User Accounts?

School district officials are responsible for providing computer network users with accounts to access resources on a school district's network. A district should have written procedures for granting, changing and disabling user access to its network. 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 or unneeded accounts as soon as there is no longer a need for them, including network user accounts of former employees.

Officials should disable unnecessary or unneeded accounts. …

The IT Director is responsible for ensuring that network user accounts are managed appropriately. 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] on the network. Also, unnecessary accounts create additional work to manage network access.

Furthermore, the IT Director should limit the number of generic accounts on the network. 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 system need.

[1] Personal, private and sensitive information (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.

District Officials Did Not Adequately Manage Network User Accounts

We reviewed all 202 nonstudent enabled network user accounts to confirm they were needed.

Unneeded Nonstudent Accounts – We compared the 202 enabled nonstudent network user accounts to the employee master list and assessed the need for the 17 nonstudent accounts that did not match the current employee list. Of the 17 accounts, we found two unneeded enabled network user accounts (12 percent) that belonged to former District employees. When we brought them to the Director's attention, he disabled them.

Unneeded network user accounts can be potential entry points for attackers. If they are not monitored or used and are accessed by an attacker, the attacker possibly could use the accounts to inappropriately access and view PPSI. Also, when a District has many network user accounts that must be managed and reviewed, unneeded network user accounts may make it more difficult to manage network access.

Unneeded Generic Accounts – Generic accounts are not linked to individual users and may be needed for certain networks services or applications to run properly. We reviewed all 26 generic accounts and inquired whether they were still needed. While it appeared that all generic accounts were used for specific purposes, District officials should know at all times who has access to and is using each account.

When numerous generic accounts are enabled on a network, officials could have difficulty managing the accounts, including disabling those that are unneeded because it may not always be clear who uses the generic accounts and whether that access is still needed. If not properly managed, generic accounts could be potential entry points for attackers, because the generic accounts could be used to inappropriately access and view PPSI on the network.

Internet browsing increases the likelihood that network users will be exposed to malware. …

How Should Officials Monitor and Enforce Compliance With the Computer Acceptable Use Policy?

To enable officials to manage and monitor network user accounts, a school district should have a computer acceptable use policy (AUP) that defines the procedures for computer, Internet and email use for network users. The policy also should describe what constitutes appropriate and inappropriate use of IT resources, the school district board's expectations concerning personal use of IT equipment and user privacy and the consequences for violating the policy.

Internet browsing increases the likelihood that network users will be exposed to malware (malicious software infections) that may compromise data confidentiality, integrity or availability. School district officials can reduce the risks to PPSI and IT assets by adopting an AUP and monitoring network users' Internet usage. District officials also should develop and implement procedures to monitor employee compliance with the AUP.

The District's computer acceptable use policy states that employees "shall refrain from using computers for personal use." The Board adopted a computer acceptable use policy stating all use of computer systems must be in support of education and/or research consistent with the District's goals and purposes. Use of the Internet for profit activity, extensive personal business or any illegal purpose is not acceptable.

Additionally, the policy states that use of the network is a privilege and may be revoked at any time for inappropriate conduct, such as abusive or objectionable language, acts of sabotage, attempts to cause congestion on the network or interfering with the work of others. The District requires all students, their parents or guardians, and staff members to sign an acceptable use contract.

Officials Did Not Monitor Compliance With the Computer Acceptable Use Policy

We examined six computers[2] to determine whether they were used for nonbusiness purposes and found evidence of personal Internet use (Figure 1).

Figure 1: Personal Internet Use

Type	Website
Personal email	Gmail.com
Social networking	Facebook.com
Shopping	Bestbuy.com
Travel	Travelocity.com
News	Msnbc.com
Entertainment	Mlb.com
Games	Play.google.com

District officials did not monitor compliance with the AUP by periodically reviewing computer website history logs for appropriateness. Instead, officials relied solely on the District's web filtering software to block prohibited websites.

According to the IT Director, the websites were not blocked by the filtering software because some employees needed access to these websites for business purposes. However, the personal use we identified was not for business purposes. For example, the Travelocity.com search was for a trip during a time when District offices were closed.

When employees access websites for nonbusiness or inappropriate purposes through the network, employee productivity is reduced. Also, the District has an increased risk that IT assets and network user information could be compromised through malware. Such information includes financial information, personnel records and student individualized education programs.

[2] Refer to Appendix B for further information on our sample selection.

What Do We Recommend?

The Board should:

1. Ensure officials monitor compliance with the AUP.

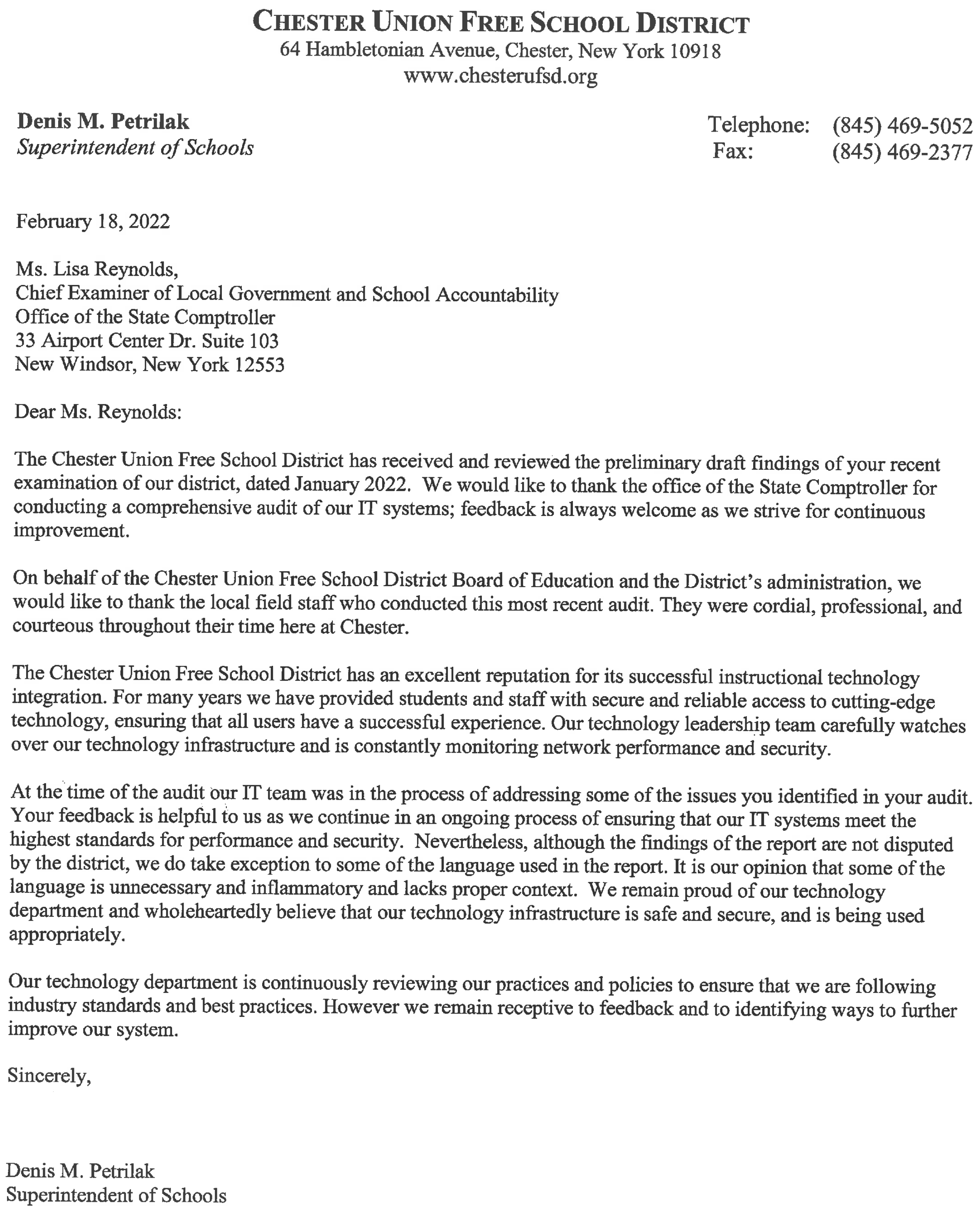
District officials should:

2. Routinely evaluate and disable any unneeded accounts.

3. Ensure all network users have and use their own unique network user accounts to access the District's network.

4. Monitor Internet use to ensure network users comply with the AUP.

Appendix A: Response From District Officials



CHESTER UNION FREE SCHOOL DISTRICT
64 Hambletonian Avenue, Chester, New York 10918
www.chesterufsd.org

Denis M. Petrilak
Superintendent of Schools

Telephone: (845) 469-5052
Fax: (845) 469-2377

February 18, 2022

Ms. Lisa Reynolds,
Chief Examiner of Local Government and School Accountability
Office of the State Comptroller
33 Airport Center Dr. Suite 103
New Windsor, New York 12553

Dear Ms. Reynolds:

The Chester Union Free School District has received and reviewed the preliminary draft findings of your recent examination of our district, dated January 2022. We would like to thank the office of the State Comptroller for conducting a comprehensive audit of our IT systems; feedback is always welcome as we strive for continuous improvement.

On behalf of the Chester Union Free School District Board of Education and the District's administration, we would like to thank the local field staff who conducted this most recent audit. They were cordial, professional, and courteous throughout their time here at Chester.

The Chester Union Free School District has an excellent reputation for its successful instructional technology integration. For many years we have provided students and staff with secure and reliable access to cutting-edge technology, ensuring that all users have a successful experience. Our technology leadership team carefully watches over our technology infrastructure and is constantly monitoring network performance and security.

At the time of the audit our IT team was in the process of addressing some of the issues you identified in your audit. Your feedback is helpful to us as we continue in an ongoing process of ensuring that our IT systems meet the highest standards for performance and security. Nevertheless, although the findings of the report are not disputed by the district, we do take exception to some of the language used in the report. It is our opinion that some of the language is unnecessary and inflammatory and lacks proper context. We remain proud of our technology department and wholeheartedly believe that our technology infrastructure is safe and secure, and is being used appropriately.

Our technology department is continuously reviewing our practices and policies to ensure that we are following industry standards and best practices. However we remain receptive to feedback and to identifying ways to further improve our system.

Sincerely,

Denis M. Petrilak
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 policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed District officials to gain an understanding of the processes and procedures for the IT system and applications.
- We ran a computerized audit script on the District's network. We then analyzed each report generated by the script, looking for weaknesses in network user account management, user privileges and group policy definition and network setting configurations.
- We used our professional judgment to select a sample of six computers from the District's 1,935 computers. We selected computers of network users who we believed had access to PPSI and financial applications. We reviewed web history reports from these computers to evaluate whether Internet use complied with the AUP. We also reviewed web history reports for accessed websites that could put the network at risk.

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.

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 Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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