DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-34

Watervliet City School District

Information Technology

JULY 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Watervliet City School District

Audit Objective

Determine whether the Watervliet City School District's (District) Board and District officials ensured information technology (IT) assets and data were safeguarded.

Key Findings

The Board and District officials did not ensure the IT assets and data were safeguarded. Officials did not:

- Establish written procedures for managing, limiting and monitoring user accounts.
- Disable 72 unneeded network accounts in a timely manner.
- Monitor compliance with the acceptable computer use policy (AUP). As a result, 12 of 13 computers we tested accessed nonbusiness websites prohibited by the policy.

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

Key Recommendations

- Review network user accounts and permissions, and disable unnecessary accounts and unneeded permissions.
- Monitor employees' Internet use to ensure compliance with the District's AUP.

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

Background

The District serves the City of Watervliet in Albany County. The District is governed by an elected five-member Board of Education (Board), responsible for the general management and control of financial and educational affairs.

The Superintendent of Schools is the District's chief executive officer and is responsible for District administration.

The Director of Educational Programs and Accountability (Director) is the network administrator responsible for the overall management of the IT infrastructure. The District contracts with Capital Region Board of Cooperative Educational Services (BOCES) to provide IT services.

Quick Facts

Network Accounts	
Total Accounts	3,132
Non-Student Accounts	421
2020-21 Appropriations	$28.6 million
Employees	209

Audit Period

July 1, 2019 – November 17, 2020

Safeguarding IT Systems

How Should District Officials Safeguard Network Access?

District officials are responsible for restricting network user access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. Operating systems and installed software programs should be updated with the most recent version from the vendor being used. This helps ensure data and IT assets, including personal, private and sensitive information (PPSI),[1] are protected from unauthorized use and access.

Network user accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating network user access with specific users. Network user accounts are potential entry points for attackers because, if compromised, they could be used inappropriately to access and view data stored on the network.

A district should have written procedures for granting, changing, updating and disabling user permissions or access to the network and to software applications. To minimize the risk of unauthorized access, officials should regularly review enabled network accounts to ensure they are still needed.

To minimize the risk of unauthorized access, officials should regularly review enabled network accounts to ensure they are still needed.

District officials should periodically compare an employee master list to the list of network user accounts to determine whether the user accounts belong to current employees and follow a process to disable unneeded accounts as soon as there is no longer a need for them. Some generic accounts may be unnecessary and can inadvertently grant users more access than needed.

Also, software on district computers should be supported and approved to be on the district's network. When vendors stop supporting certain software versions, they may stop providing technical support or bug and security fixes (patches) for those versions. Without ongoing updates, security weaknesses and bugs in the software can be exploited by attackers in a wide range of ways.

Additionally, software installed on district computers that is not on the approved list may not be updated regularly because IT staff is unaware of its existence. Officials should ensure that all software is up-to-date and supported by vendors and only software on the approved list is installed.

Officials Did Not Adequately Safeguard the Network

Network Accounts – District officials have not established written procedures for managing, limiting and monitoring user accounts. The IT vendor is notified verbally or through email when changes need to be made to a user's access.

[1] PPSI is any information to which unauthorized access, disclosure, modification or destruction – or disruption of access or use – could have or cause severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

We examined all 421 non-student network user accounts to determine whether the accounts were active, assigned to current employees or third-party contractors, or an appropriate generic account, and had proper user permissions. We determined 72 (17 percent) of these network user accounts were unnecessary and were not disabled in a timely manner.[2] In addition, three of these accounts had unneeded administrative permissions. The 72 user accounts included:

- 30 generic network user accounts that are not assigned to specific users.
- 27 accounts associated with former employees or third-party contractors.
- 15 accounts related to software or other processes that were no longer used.

The District's network was more vulnerable to cybersecurity attacks because unused and unneeded network accounts were not removed in a timely manner. User accounts of former employees that had not been disabled could potentially be used by those individuals or others for malicious purposes.

District officials told us they thought the current process of removing and adding accounts as needed was sufficient. Because the District did not have procedures to regularly review enabled network user accounts to identify and disable unneeded accounts, the unneeded user accounts went unnoticed until our audit and were inadequately managed. In addition, because the District's network had unused, unneeded active network user accounts, it had a greater risk that these accounts could be used as entry points for attackers to access and compromise IT resources.

How Does an AUP Secure and Protect a District's IT Systems?

A school district should have an AUP policy that defines the procedures for computer, Internet and email use. The policy should also describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy.

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by monitoring Internet use and configuring web filtering software to block access to unacceptable websites and help limit access to sites that comply with the AUP. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, AUPs or standard security practices.

[2] Refer to Appendix B for information on our methodology.

Monitoring for AUP compliance involves reviewing and analyzing Internet browsing; regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity; and investigating and reporting such activity. Automated mechanisms may be used to perform this process and can help security professionals routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access.

In addition, officials should require employees to sign acknowledgement forms to indicate that they read the AUP and were aware what was expected of them, and to acknowledge they would be held accountable to the policies and procedures outlined in the AUP.

Officials Did Not Monitor AUP Compliance

The District's AUP requires IT users to sign an acknowledgement form indicating that they are aware of and will comply with the District's AUP. However, officials did not monitor employee Internet use or implement procedures to monitor compliance with the AUP. We reviewed the web browsing history on the 13 computers used by key District officials with access to PPSI. We found that 12 of these computers had a history of visiting websites prohibited by the AUP.

Specifically, users accessed websites for personal purposes, such as shopping, banking and travel, and other non-District related activities, such as watching videos or browsing entertainment news and blogs. Also, officials did not implement any controls to prevent users from accessing non-work related websites, such as installing web filtering software to prevent access to these websites. Further, these officials should have been aware their Internet use did not comply with the AUP. Our review of the signed acknowledgement forms indicated they had read and agreed to abide by the AUP. There was no monitoring of web activity because District officials relied on a content filter, which only blocked access to obscene, violent and other specifically identified websites that did not comply with the AUP.

...[U]sers accessed websites for personal purposes, such as shopping, banking and travel...

By allowing personal use of District computers, the District had an increased risk that its network and computers would be exposed to attacks and malicious software that may compromise PPSI and the network. Additionally, the combination of unrestricted web browsing and outdated software increased the risk that malicious software attacks could be successful. As a result the District's IT assets and any PPSI they contain had a higher risk of exposure to damage and PPSI breach, loss or misuse. Further, employee time and other resources used for personal activities instead of District business was an inefficient use of taxpayer funds.

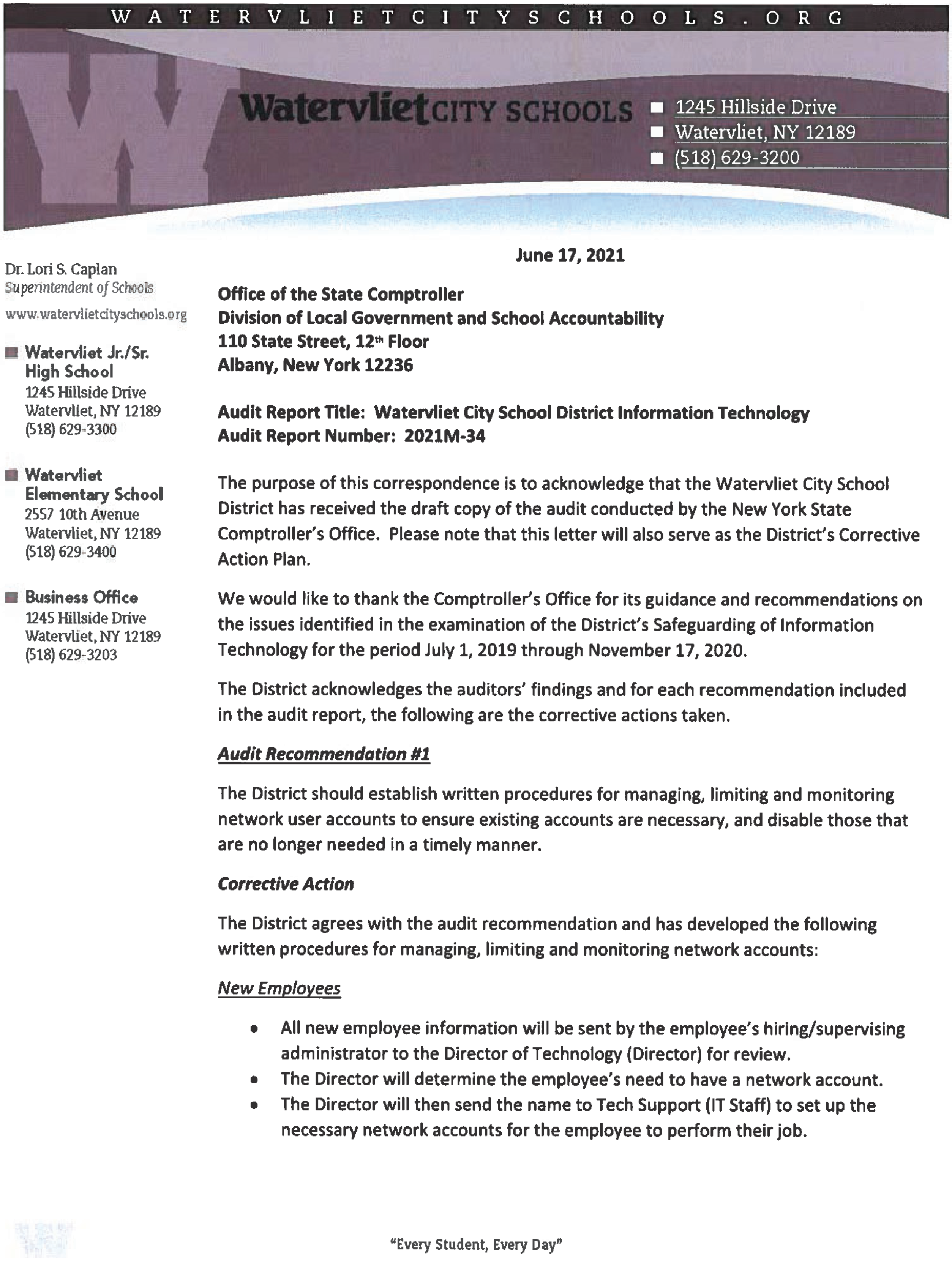
What Do We Recommend?

District officials should:

1. Establish written procedures for managing, limiting and monitoring network user accounts to ensure existing accounts are necessary, and disable those that are no longer needed in a timely manner.

2. Implement procedures to monitor compliance with the AUP.

Appendix A: Response From District Officials



WATERVLIETCITYSCHOOLS.ORG

Watervliet CITY SCHOOLS

- 1245 Hillside Drive
- Watervliet, NY 12189
- (518) 629-3200

Dr. Lori S. Caplan
Superintendent of Schools
www.watervlietcityschools.org

Watervliet Jr./Sr. High School
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3300

Watervliet Elementary School
2557 10th Avenue
Watervliet, NY 12189
(518) 629-3400

Business Office
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3203

June 17, 2021

Office of the State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor
Albany, New York 12236

Audit Report Title: Watervliet City School District Information Technology
Audit Report Number: 2021M-34

The purpose of this correspondence is to acknowledge that the Watervliet City School District has received the draft copy of the audit conducted by the New York State Comptroller's Office. Please note that this letter will also serve as the District's Corrective Action Plan.

We would like to thank the Comptroller's Office for its guidance and recommendations on the issues identified in the examination of the District's Safeguarding of Information Technology for the period July 1, 2019 through November 17, 2020.

The District acknowledges the auditors' findings and for each recommendation included in the audit report, the following are the corrective actions taken.

Audit Recommendation #1

The District should establish written procedures for managing, limiting and monitoring network user accounts to ensure existing accounts are necessary, and disable those that are no longer needed in a timely manner.

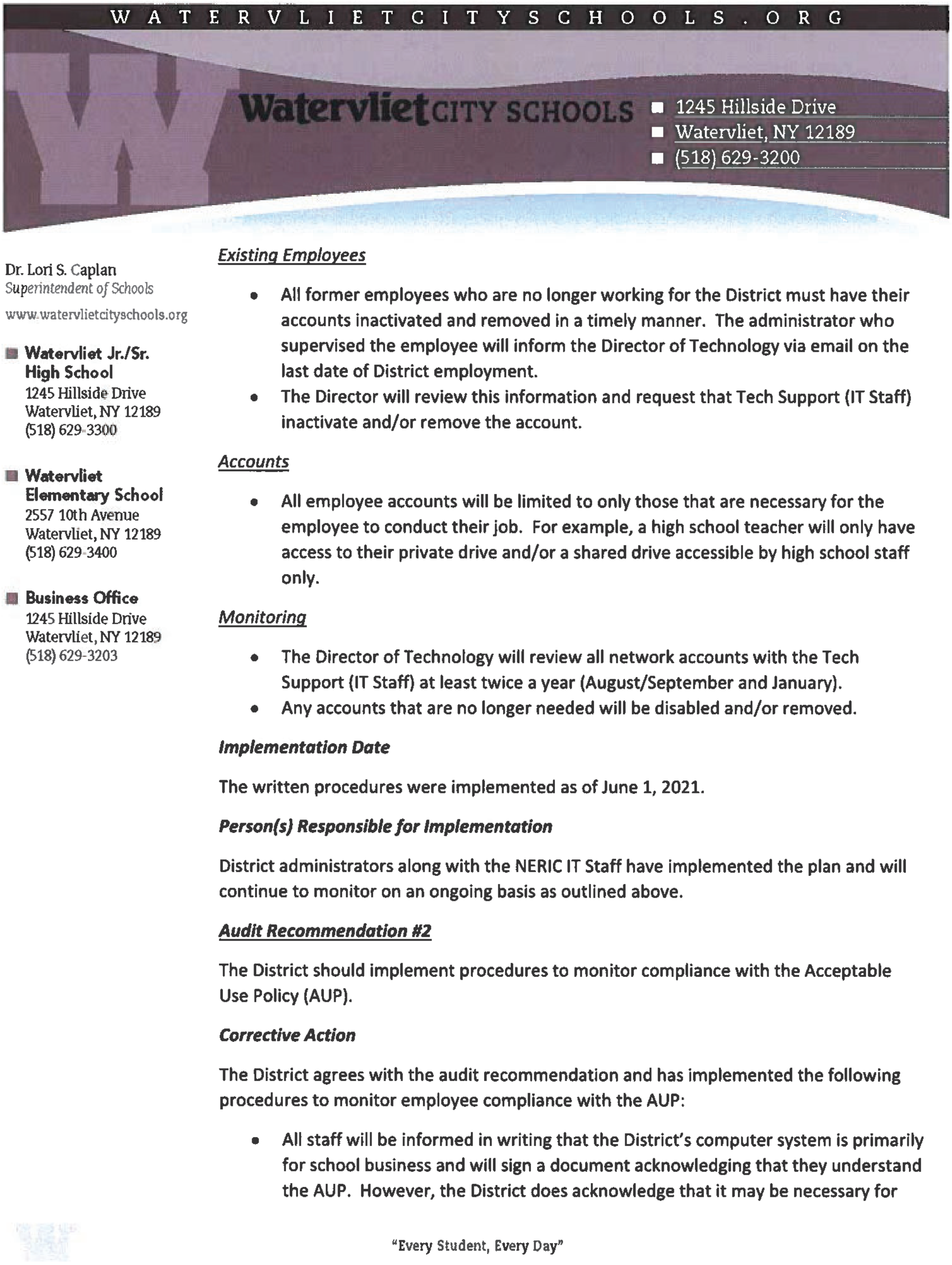
Corrective Action

The District agrees with the audit recommendation and has developed the following written procedures for managing, limiting and monitoring network accounts:

New Employees

- All new employee information will be sent by the employee's hiring/supervising administrator to the Director of Technology (Director) for review.
- The Director will determine the employee's need to have a network account.
- The Director will then send the name to Tech Support (IT Staff) to set up the necessary network accounts for the employee to perform their job.

"Every Student, Every Day"



Dr. Lori S. Caplan
Superintendent of Schools
www.watervlietcityschools.org

Watervliet Jr./Sr. High School
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3300

Watervliet Elementary School
2557 10th Avenue
Watervliet, NY 12189
(518) 629-3400

Business Office
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3203

Existing Employees

- All former employees who are no longer working for the District must have their accounts inactivated and removed in a timely manner. The administrator who supervised the employee will inform the Director of Technology via email on the last date of District employment.
- The Director will review this information and request that Tech Support (IT Staff) inactivate and/or remove the account.

Accounts

- All employee accounts will be limited to only those that are necessary for the employee to conduct their job. For example, a high school teacher will only have access to their private drive and/or a shared drive accessible by high school staff only.

Monitoring

- The Director of Technology will review all network accounts with the Tech Support (IT Staff) at least twice a year (August/September and January).
- Any accounts that are no longer needed will be disabled and/or removed.

Implementation Date

The written procedures were implemented as of June 1, 2021.

Person(s) Responsible for Implementation

District administrators along with the NERIC IT Staff have implemented the plan and will continue to monitor on an ongoing basis as outlined above.

Audit Recommendation #2

The District should implement procedures to monitor compliance with the Acceptable Use Policy (AUP).

Corrective Action

The District agrees with the audit recommendation and has implemented the following procedures to monitor employee compliance with the AUP:

- All staff will be informed in writing that the District's computer system is primarily for school business and will sign a document acknowledging that they understand the AUP. However, the District does acknowledge that it may be necessary for

"Every Student, Every Day"

WATERVLIETCITYSCHOOLS.ORG

Watervliet CITY SCHOOLS
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3200

Dr. Lori S. Caplan
Superintendent of Schools
www.watervlietcityschools.org

Watervliet Jr./Sr. High School
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3300

Watervliet Elementary School
2557 10th Avenue
Watervliet, NY 12189
(518) 629-3400

Business Office
1245 Hillside Drive
Watervliet, NY 12189
(518) 629-3203

staff to occasionally use the system for incidental personal use and will adjust the AUP accordingly.

- Due to the increasing number of cybersecurity threats, employees will not use the District's computer system to access their personal email accounts. If necessary, employees should only utilize their personal devices (i.e. cell phones) to access their email while in the work place.
- The District will continue to use content filtering software to block software and websites that the District has deemed inappropriate or has the potential to harbor malware or other cybersecurity threats.
- The NERIC IT Staff will monitor staff browsing history on an ongoing basis and report any suspected inappropriate use to the Director of Technology.

Implementation Date

The written procedures were implemented as of June 1, 2021.

Person(s) Responsible for Implementation

District administrators along with the NERIC IT Staff have implemented the plan and will continue to monitor employee compliance on an ongoing basis as outlined above.

This Corrective Action Plan addresses all of the recommendations included in the Comptroller's report. We would like to thank the Comptroller's Office for its thorough work and invite the Comptroller's staff to return and examine the improvements that the District has implemented.

Respectfully submitted,

Amanda Cavanaugh, President
Watervliet City School District Board of Education

Cc: New York State Education Department
Office of Audit Services, Room 524 EB
89 Washington Avenue
Albany, NY 12234

Dr. Lori S. Caplan, Superintendent
Watervliet City School District

"Every Student, Every Day"

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 and BOCES personnel and reviewed the District's policy manual to gain an understanding of the District's IT environment and internal controls.
- We analyzed network user accounts and settings using a computerized audit script. We compared the 421 nonstudent enabled network accounts to the active employee list and interviewed District officials to identify accounts of former employees and/or unauthorized users.
- We used our professional judgment to select a sample of 13 employee computers. We selected computers of users who had access to PPSI data. We ran computerized audit scripts on these computers and the server to identify a list of installed software.
- We used our professional judgment to select a sample of the most frequently used 50 software titles and reviewed our sample to determine whether the most current software versions were installed. We also compared our sample to the District's approved software list to determine whether any installed software was not approved.
- We used computerized audit scripts to review web histories on our sample of 13 computers. We reviewed sites visited 150 times or more to determine whether there was any personal, questionable, or inappropriate Internet use and the websites complied with the AUP.

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
https://www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://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
https://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
https://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
https://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

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

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