DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-154

Putnam Valley Central School District

Information Technology

JANUARY 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights 1

Information Technology 2

How Should IT Systems Be Secured and Protected? 2

Officials Did Not Adopt a Password Security Policy 2

Officials Did Not Adequately Manage Administrative Account Use . . 3

What Do We Recommend? 4

Appendix A – Response From District Officials 5

Appendix B – Audit Methodology and Standards 7

Appendix C – Resources and Services. 9

Report Highlights

Putnam Valley Central School District

Audit Objective

Determine whether Putnam Valley Central School District's (District) officials ensured information technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

District officials did not ensure IT systems were adequately secured and protected against unauthorized use, access and loss. Officials did not adopt a password security policy or manage the use of administrative accounts. As a result, the District has an increased risk of unauthorized use or access that could result in important data loss and a serious interruption in operations. Officials did not:

- Adopt an adequate password security policy to address password requirements.
- Create secondary user accounts for the IT system for three employees whose job responsibilities required administrative permissions, to be used for non-administrative activities.

In addition, sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive password security policy to address password requirements.
- Assess all local user accounts with administrative permissions and create secondary accounts to be used for non-administrative activities.

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

Background

The District serves the Towns of Putnam Valley and Carmel in Putnam County and the Town of Cortlandt in Westchester County.

The District is governed by an elected five-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 Director of Technology and CIO (IT Director) is responsible for managing the District's IT systems including network security and user accounts.

The District relies on its IT assets for Internet access, email and maintaining confidential and sensitive financial, student and personnel records.

Quick Facts	
Local User Accounts	2,626
Employees	502
Student Enrollment	1,595

Audit Period

July 1, 2019 – May 31, 2021. We extended the audit period forward through July 28, 2021 to complete IT testing.

Information Technology

If IT assets are compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of an IT system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by unauthorized access and use.

> … [A] lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by unauthorized access and use.

How Should IT Systems Be Secured and Protected?

IT security policies describe the tools and procedures used to help protect data and IT systems, define district officials' expectations for appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential that a board establish security policies for key IT security issues including those related to user accounts and permissions, disseminate the policies to officials, staff and students, and ensure officials monitor and enforce the policies. Further, a board should periodically review these policies, update them as needed, designate personnel who are responsible for monitoring policy compliance and communicate the policies to all users.

User accounts provide access to a district's computer resources 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, modify, corrupt or delete personal, private and sensitive information (PPSI)[1] on the system.

District officials should restrict user access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT systems are secure from unauthorized use and/or modification.

To minimize the risk of unauthorized access, district officials should actively manage user accounts and permissions, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized.

Officials Did Not Adopt a Password Security Policy

While District officials developed and the Board adopted policies addressing most key IT security issues, they have not developed and adopted a password security policy. Although the Board did not formally adopt a password security policy, the District has a password guidance document that the IT Director believed to be sufficient. However, because this policy was not adopted by Board resolution,

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

it may not carry the Board's authority when it is necessary to enforce the consequences of violation.

District officials cannot be certain that the confidentiality, integrity and availability of data and computer systems are protected without developing and implementing adequate password policies and procedures to ensure users, or those who manage IT, understand these policies and procedures and their roles and responsibilities related to IT and data security. When there are inadequate policies to clearly describe the consequences of policy violations, enforcing any such policies may be difficult and the system, data and PPSI could be at a greater risk for unauthorized access, loss or misuse.

Officials did not have secondary lesser-privileged user accounts for IT administrators.

Officials Did Not Adequately Manage Administrative Account Use

Officials did not have secondary lesser-privileged user accounts for IT administrators. We reviewed the permissions granted to all the 30 local user accounts on 11 computers and examined them for necessity and appropriateness.[2]

Three administrators (all District employees) had local user accounts with administrative permissions but did not have separate, lesser-privileged accounts to be used as needed to fulfill their job responsibilities for non-administrative functions such as browsing the Internet and checking email. The IT Director told us, and we confirmed that these are local accounts that only have access to the individual computers assigned to the user and are therefore not considered administrative accounts to access other programs. However, this does not reduce the risk that the system becomes inadvertently exposed to malicious software (malware) during Internet browsing or email access, and this could result in greater damage than if lesser-privileged accounts were used for those activities.

A user with administrative permissions could be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website, or accessing a website programmed to automatically infect the user's computer with malware. If a deceived user has administrative permissions, the attacker could cause greater damage than with a lesser privileged account.

Without assigning and providing a separate non-administrative local user account for routine activities that do not require administrative permissions, the District is at a significantly greater risk of unauthorized access and loss of resources including PPSI due to inadvertent exposure of the system to malware during Internet browsing or email access. Further, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

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

What Do We Recommend?

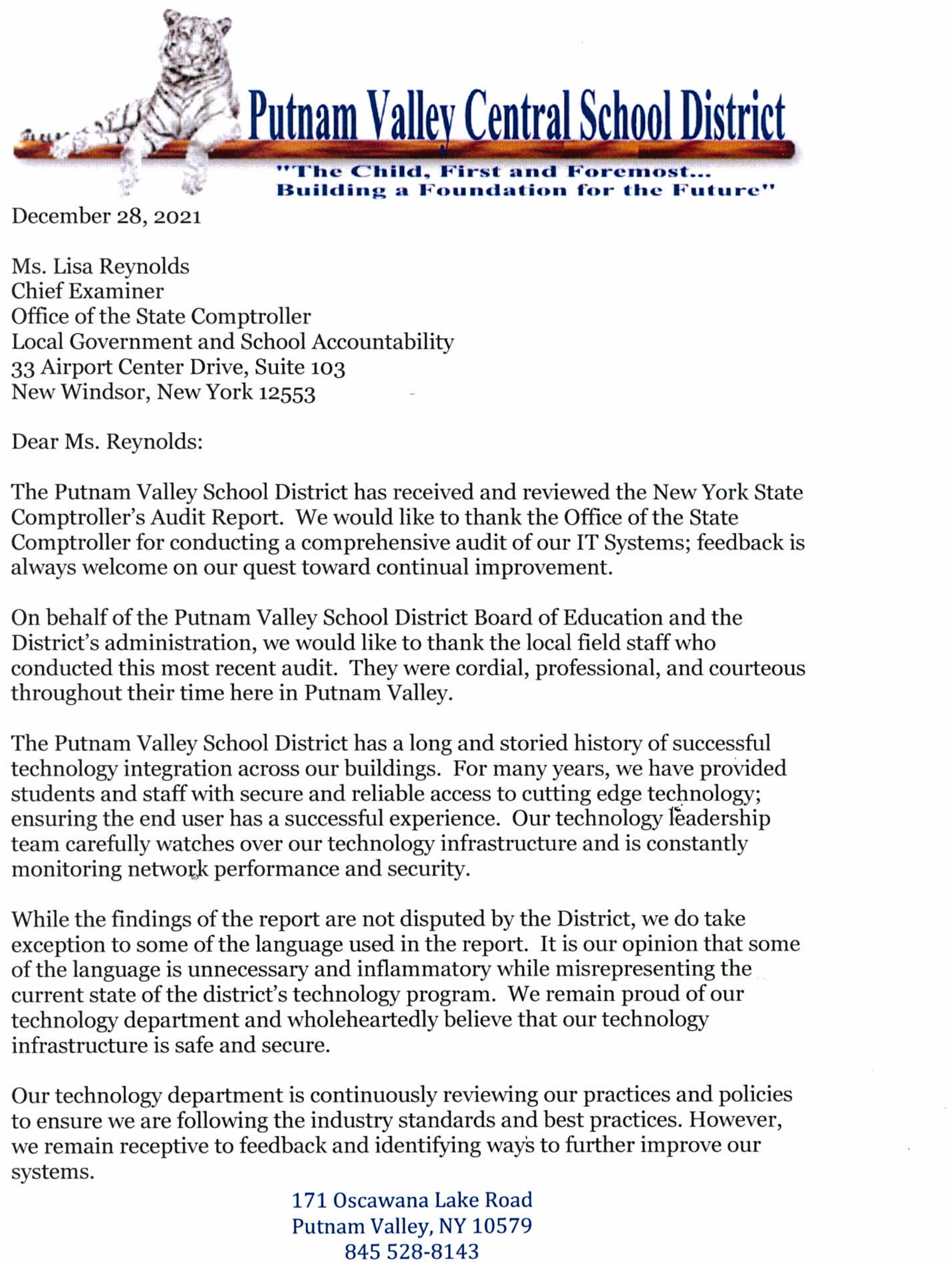
The Board should:

1. Adopt a comprehensive password security policy to address password requirements and to communicate expectations to District officials and employees.

The IT Director should:

2. Ensure that all employees with administrative account access have and use a dedicated or secondary account for activities that do not require elevated access.

Appendix A: Response From District Officials



Putnam Valley Central School District

"The Child, First and Foremost...
Building a Foundation for the Future"

December 28, 2021

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

Dear Ms. Reynolds:

The Putnam Valley School District has received and reviewed the New York State Comptroller's Audit Report. We would like to thank the Office of the State Comptroller for conducting a comprehensive audit of our IT Systems; feedback is always welcome on our quest toward continual improvement.

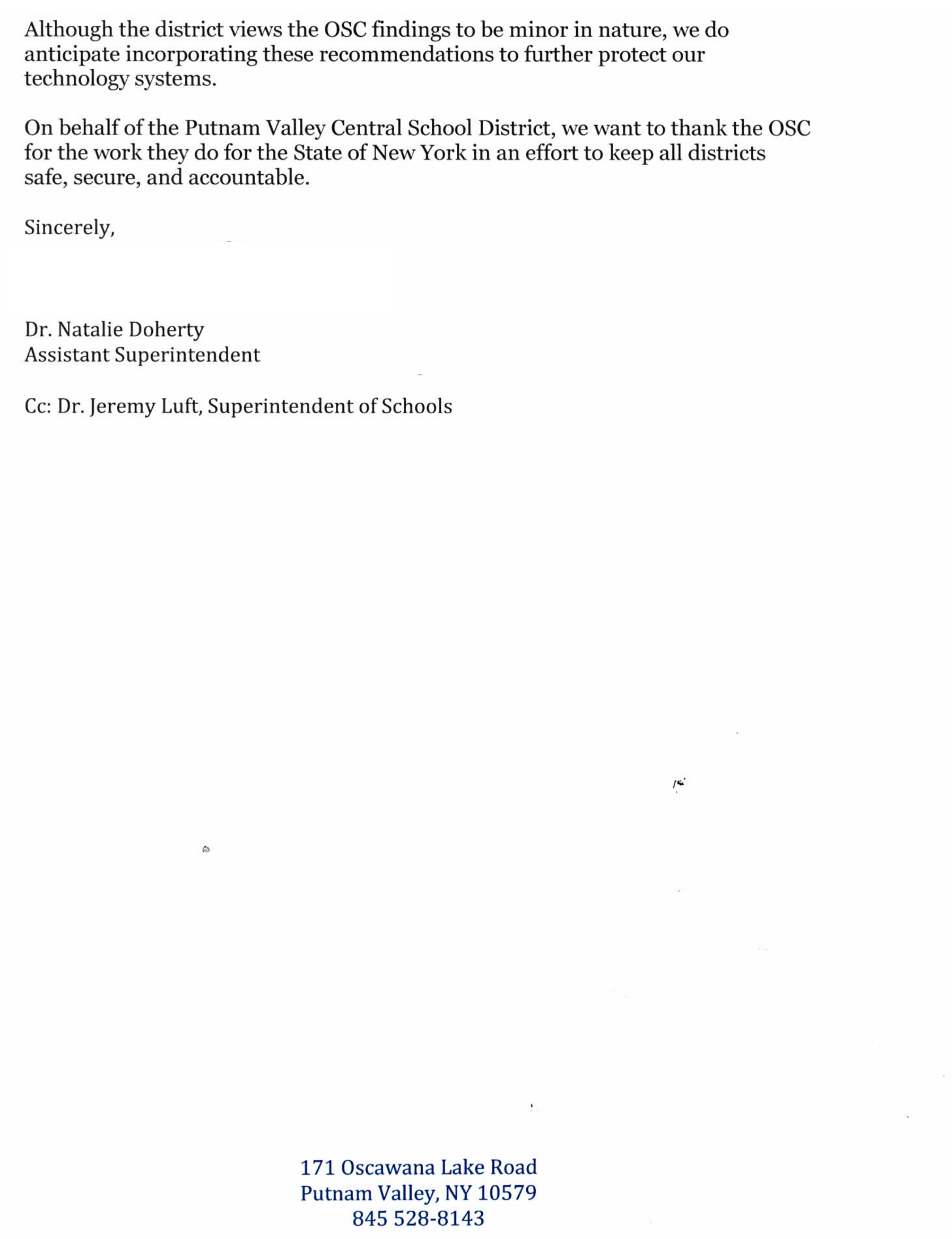
On behalf of the Putnam Valley School District Board of Education and the District's administration, we would like to thank the local field staff who conducted this most recent audit. They were cordial, professional, and courteous throughout their time here in Putnam Valley.

The Putnam Valley School District has a long and storied history of successful technology integration across our buildings. For many years, we have provided students and staff with secure and reliable access to cutting edge technology; ensuring the end user has a successful experience. Our technology leadership team carefully watches over our technology infrastructure and is constantly monitoring network performance and security.

While 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 while misrepresenting the current state of the district's technology program. We remain proud of our technology department and wholeheartedly believe that our technology infrastructure is safe and secure.

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

171 Oscawana Lake Road
Putnam Valley, NY 10579
845 528-8143



Although the district views the OSC findings to be minor in nature, we do anticipate incorporating these recommendations to further protect our technology systems.

On behalf of the Putnam Valley Central School District, we want to thank the OSC for the work they do for the State of New York in an effort to keep all districts safe, secure, and accountable.

Sincerely,

Dr. Natalie Doherty
Assistant Superintendent

Cc: Dr. Jeremy Luft, Superintendent of Schools

171 Oscawana Lake Road
Putnam Valley, NY 10579
845 528-8143

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 and reviewed the District's IT related policies and procedures to gain an understanding of the IT environment and internal controls.
- We used our professional judgment to select a sample of 11 computers from the District's 78 computers of users who had access to PPSI. We examined these computers using a computerized audit script ran on July 28, 2021 to determine whether user accounts had administrative permissions and assess the related security settings applied to the accounts. We analyzed each report generated by the script to identify weaknesses in user account management, privilege and group definitions.
- We ran a computerized audit script on July 28, 2021 on each of these selected 11 computers that retrieved installed software and internally accessible services (i.e., open ports). We reviewed the software versions to determine whether they were supported.
- We inquired whether District officials and personnel received IT security awareness training.

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: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Sullivan, Ulster,
Westchester counties

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