REPORT OF EXAMINATION | 2020M-154

Valley Central School District

Information Technology

JUNE 2021

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

Contents

Report Highlights

Valley Central School District

Audit Objective

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

Key Findings

The Board and District officials did not ensure IT systems were adequately secured and protected.

- District officials did not monitor compliance with the District's computer acceptable use policy.
- The District did not have a contingency plan to recover in the event of a significant service interruption.
- The Board did not physically control access to or establish environmental controls over the server room.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Monitor compliance with the computer acceptable use policy.
- Adopt a contingency plan so that users know their duties during a significant service interruption.
- Establish physical security and environmental controls over the server room.

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

Background

The District is located in the towns of Crawford, Hamptonburgh, Montgomery, Newburgh and New Windsor in Orange County and the towns of Shawangunk and Wallkill in Ulster County.

The District is governed by the Board, which is composed of seven elected members.

The Superintendent is appointed by the Board and is responsible for day-to-day management.

The IT Director is responsible for all IT functions and manages all IT infrastructure.

Quick Facts	
Total Network User Accounts	5,053
Nonstudent Network Accounts	696

Audit Period

July 1, 2018 – November 13, 2020. We extended the audit scope through July 8, 2020 to complete our IT testing.

Information Technology

IT systems and data are valuable resources. The District relies on its IT assets for Internet access, for email and for maintaining financial, personnel and student records. If the 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 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.

What Are Effective IT Controls?

An acceptable use policy should be developed to describe what constitutes appropriate and inappropriate use of IT resources, along with the Board's expectations concerning personal use of IT equipment and user privacy. The District's computer use policy states that employees shall refrain from using computers for personal use.

A contingency plan should be developed to provide a framework for reconstructing vital operations to resume time-sensitive operations and services after a significant service interruption. A disruptive event could include a major natural disaster such as a flood, or something smaller, such as malfunctioning software. The disruptive event may compromise the availability or integrity of an IT system and data. Typically, planning for an event includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions to maintain or quickly resume operations. The plan should be tested periodically and updated to ensure it works as intended and officials understand their roles and responsibilities in a disaster situation.

Officials Did Not Monitor Compliance With the Computer Use Policy

The Board adopted an acceptable use policy stating employees shall refrain from using computers for personal use, including but not limited to shopping for products and services and making travel reservations, and that employees must not have an expectation of privacy in the use of the District's computers. However, officials did not enforce the policy and have not designed and implemented procedures to monitor compliance with the policy.

The District's …policy states that employees shall refrain from using computers for personal use... including but not limited to shopping for products and services and making travel reservations…

We examined 10 computers to determine whether they were used for nonbusiness purposes and found evidence of personal use on eight computers (Figure 1). Such use included the following:

Figure 1: Examples of Personal Internet Use

Type	Site
Personal Email	Webmail.spectrum.net
Social Networking	Snapchat.com
Shopping	Kohls.com
Travel	Oceancityvacation.com
News/Entertainment	Goodhousekeeping.com
Music	Siriusxm.com
Personal Online Banking	Hvfcu.org

According to officials, they were unable to monitor compliance with the policy due to a lack of personnel. When employees access websites for nonbusiness or inappropriate purposes through the network, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections (malware).

The Board Did Not Adopt a Contingency Plan

District officials have not formally identified, documented and prioritized threats to the IT system and data. Additionally, officials have not developed a written contingency plan that provides instructions as to how employees should communicate, where they will go and how they will perform their jobs to recover in the event of a significant IT service disruption.

According to officials, the development of a plan has been delayed due to a lack of personnel and funds. Without a plan, in the event of a disruption, the District has no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data vital for District operations. Furthermore, essential employees may not be aware of their role, increasing the time and financial resources necessary to recover from an incident.

What Are Effective Physical Controls?

Physical security controls restrict physical access to computer resources to those who need access and protect these resources from unauthorized access, intentional or unintentional harm, loss or impairment. Server rooms and wiring closets should be locked, with only necessary IT personnel having access to the keys, in order to prevent unauthorized individuals gaining access to servers and potentially to sensitive muni data. Additionally, logs of the access to server rooms and wiring closets should be maintained in order to keep accurate records

and accountability in the event that there is a problem in one of these areas. Environmental controls such as a cooling system and temperature controls, smoke detectors, fire alarms and extinguishers, and protection from water damage should be created to reduce the possibility of environmental hazards and prevent the equipment from being destroyed. Additionally, an uninterruptible dedicated power supply should be utilized to enable equipment to continue to be used and/or be properly shut down.

Officials Did Not Physically Control the Server Room

The District's server room is accessible to all employees who have a District master key. However, many of the employees who can access the server room do not need access. Employees with the master key include most District officials and janitorial staff. Further, there is no log of entry or keypad to enter the server room. The server room has no cooling system or temperature control, just a manually controlled air conditioner. Additionally, there is no fire suppression system in the room. Although the District's server is on a battery backup, the server is not on a designated generator.

According to officials, IT improvement upgrades are limited due to limited financial resources. As a result of poor physical security controls and the absence of a dedicated source of reliable power, there is a significantly greater risk of IT assets being compromised by internal, external or environmental factors, resulting in an interruption of service.

What Do We Recommend?

The Board should:

1. Ensure officials monitor compliance with the computer acceptable use policy.
2. Adopt a written contingency plan that provides instructions as to how employees should communicate, where they will go and how they will perform their jobs in the event of a significant service interruption and identifies the types of threats to the IT system.

The IT Director should:

3. Monitor Internet use to ensure employees comply with the acceptable use policy.
4. Create a contingency plan, and test and update the plan periodically to ensure it works as intended and that users know their duties during a significant service interruption.

5. Establish physical security and environmental controls over the server room to protect IT systems and resources. Such controls include limiting key access to the room, maintaining a log of entry and installing a cooling system and temperature control, a fire suppression and a dedicated uninterruptible power supply.

Appendix A: Response From District Officials

VALLEY CENTRAL SCHOOL DISTRICT
ADMINISTRATION OFFICES
944 STATE ROUTE 17K
MONTGOMERY, NY 12549-2240
PHONE: (845) 457-2400 Ext. 18510
www.vcsd.k12.ny.us

OFFICE OF THE
SUPERINTENDENT

JOHN P. XANTHIS

May 25, 2021

Office of the New York State Comptroller
Newburgh Regional Office
Lisa A. Reynolds, Chief Examiner
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Dear Chief Examiner Reynolds,

The Valley Central School District is in receipt of Report of Examination 2020M-154 and responds to the findings as follows:

Officials Do Not Monitor Compliance with the Computer Use Policy
District officials will review the Computer Use Policy with all staff and will develop a corrective action plan to monitor for compliance going forward.

The Board Did Not Adopt a Contingency Plan
District officials will work with outside agencies to identify, document, and prioritize threats to the IT system and infrastructure. The District's corrective action plan will include the development of a written contingency plan.

Officials Did Not Physically Control the Server Room
District officials will secure and limit access to the server room. As part of the District's corrective action plan, District officials will consult with the District's Engineer to evaluate the cooling system and a fire suppression system in the District's server room.

District officials thank the Examiner's office for its thorough and professional audit which began in November of 2019.

Sincerely,

John P. Xanthis
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 user account management, privilege and group definition and network setting configurations.
- We used our professional judgment to select a sample of 10 computers from the District's 8,924 computers. We selected computers of users who had access to PPSI[1] and software programs with known vulnerabilities. We reviewed web history reports from these computers to evaluate whether Internet use complied with the acceptable use policy. We also reviewed web history reports for accessed websites that could put the network at risk.
- We performed a walk-through of the District to identify any weaknesses in the physical security controls over IT systems and devices and to obtain an understanding of the systems and their functionalities.

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.

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.

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

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, Ulster, Westchester counties

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