REPORT OF EXAMINATION | 2022M-64

Sodus Central School District

Software Management

NOVEMBER 2022

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

Contents

Report Highlights

Sodus Central School District

Audit Objective

Determine whether Sodus Central School District (District) officials ensured only appropriate, necessary and authorized software was installed on District computers.

Key Findings

District officials did not establish adequate controls to prevent inappropriate, unnecessary and unauthorized software from being installed on District computers. As a result, we found:

- All 39 network user accounts that we reviewed had permissions that allowed the accounts' users to install software on their computers without authorization.
- Of 134 software applications that we reviewed, only three (2 percent) were listed on the District's software inventory and 27 (20 percent) were unneeded or did not have a specific business purpose, including eight unauthorized software applications on 17 different computers.

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

Key Recommendations

- Limit permissions for installing software to users who need these permissions to perform their job duties and responsibilities.
- Maintain a complete and comprehensive software inventory list of all authorized, appropriate and necessary software installed on District computers.
- Establish comprehensive written procedures for installing and periodically reviewing software on District computers.

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

Background

The District serves the Towns of Arcadia and Sodus in Wayne County. The District is governed by a seven-member Board of Education (Board) that is responsible for managing and controlling the District's educational and financial affairs.

The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The Director of Personalized Learning and Innovative Technology (Director), who also is the District's data protection officer, oversees the District's Information Technology (IT) Department.

Quick Facts	
2021-22 IT Department Appropriations	$201,842
Total Desktops and Laptops	620
Total Staff	342
Total Non-Student Network User Accounts	486

Audit Period

July 1, 2020 – February 1, 2022

Software Management

How Should Officials Manage Installed Software on District Computers to Ensure It Is Appropriate, Necessary and Authorized?

IT staff should install only appropriate, necessary and authorized software on school district computers. This helps reduce the risk of unwanted consequences and unnecessary costs that could result from allowing users to install unauthorized software, such as potentially causing a network failure, opening the school district's network to attack and/or causing loss of productivity by allowing users to use nonbusiness-related applications during work hours.

School district officials should be aware, and understand the use, of software installed on school district computers and how best to track it. IT managers can track software, in part, by maintaining complete and accurate detailed inventory records of authorized, appropriate and necessary software installed on computers. Inventory records should include a description of the software, description of the computer(s) on which the software is installed and any pertinent licensing information.

School district officials should be aware, and understand the use, of software installed on school district computers. ...

Furthermore, school district officials should establish and implement comprehensive written procedures that require IT staff to monitor or review computers to identify installed software and remove any inappropriate, unnecessary and unauthorized software. IT staff also should limit permissions on user accounts to the least privileges necessary for users to perform daily tasks. Restricting these permissions would help to limit the risk exposure that inappropriate, unnecessary and unauthorized software downloads and/or installations could cause.

The District Did Not Maintain a Complete Inventory of All Authorized and Installed Software

Although the IT Department maintained an inventory of software used by District users, it consisted primarily of software used for educational purposes and did not include all authorized software installed on District computers. We reviewed 65 computers[1] and found 134 software applications. Of the 134 software applications, we found that only three (2 percent) were included in the District's software inventory. District officials indicated that most of these exceptions were necessary, appropriate and authorized software but they were not properly inventoried.

The Director and District officials did not establish written policies and procedures for reviewing or monitoring installed software on computers. Therefore, IT staff did

1 Refer to Appendix B for further information on our sample selection.

not regularly review software installations on District computers or restrict users from installing software on computers.[2]

IT staff did not periodically review software installations because it was not standard practice for them to regularly collect computers from staff and they did not implement another method to monitor software installations. In addition, IT staff did not restrict permissions for installing software because it was a long-standing District practice to allow these permissions. However, it is a long-standing and widely-accepted IT security control to restrict permissions for installing software.

Because IT staff did not maintain a complete software inventory list or restrict permissions to prevent non-IT staff from installing software on District computers, we found unauthorized software installed on 17 computers. Furthermore, because IT staff did not regularly review software installations, the unauthorized software that we found remained undetected until our audit.[3]

IT staff told us that some of the District's software vendors use cloud-based controls to track software licenses, which helps ensure that the District has purchased a sufficient number of licenses. However, IT staff should still ensure that the District has purchased enough software licenses to comply with copyright laws. Additionally, while cloud-based controls may assist officials in tracking software licenses, officials still are responsible for actively monitoring all software applications installed on District computers to help ensure they are appropriate, necessary and authorized.

District Officials Did Not Implement Appropriate Procedures to Monitor Software

The Board adopted a staff acceptable use policy (AUP) to provide users with guidelines for IT asset use and security. The policy authorizes the use of the District's computer system and computers only for work-related purposes. It states that staff "will adhere to laws, policies and rules governing computers and software."

The policy authorizes the use of the District's computer system and computers only for work-related purposes.

While the AUP requires staff to agree to the AUP's terms in writing, District officials told us that this was not currently being enforced, but did not give a specific reason why it was not enforced. As a result, District officials could not ensure that staff was informed of the Board's AUP expectations, specifically as it related to software installations on District computers.

2 Refer to the District Officials Did Not Implement Appropriate Procedures to Monitor Software section for further information.
3 Ibid.

We reviewed 65 computers[4] that had 134 software applications installed on them to determine whether installed software was authorized, was for a legitimate business purpose and complied with the District's AUP. Of the 134 applications, we found that 27 did not have a specific business or academic use. These applications included 19 unneeded preinstalled software installed by the computer vendors and eight unauthorized software applications on 17 different computers (installed by non-IT staff) that did not have a business purpose or were inappropriate because the District did not own a license for the software. These unauthorized applications included software related to personal tax preparation, personal smartphones or watches and bookkeeping software that was unrelated to the District.

In addition, we found that all 39 network user accounts, associated with users assigned to the 65 computers reviewed, had permissions that allowed users to download and install software on the computers. Nine of the users who had accounts with these elevated permissions had unnecessary software on their computers.

Because staff were granted unneeded permissions to install software on their computers and because IT staff did not thoroughly and regularly monitor installed software, these unnecessary and inappropriate software installations – and potential violations of the District's AUP – went undetected until our audit.

As a result, the District has an increased risk that unauthorized software, including malicious software (malware), could be installed and remain undetected. Malware can gather sensitive information such as passwords without a computer user's knowledge, corrupt data or delete files, make devices inaccessible or inoperable, be expensive to fix and can cause significant losses in productivity until corrected. Furthermore, because officials did not require users to formally accept the AUP's terms, they may be limited while attempting to enforce the AUP.

What Do We Recommend?

The Director, District officials and IT staff should:

1. Maintain a complete and comprehensive software inventory list of all authorized, appropriate and necessary software applications installed on District computers.

2. Regularly examine computers, review software installations and uninstall any inappropriate, unnecessary and unauthorized software.

4 See supra, note 1.

3. Establish comprehensive written policies and procedures for reviewing software on District computers and monitoring software licenses.
4. Limit permissions for installing software to users who need these permissions to perform their job duties and responsibilities.
5. Ensure all users agree to the AUP's terms in writing.

Appendix A: Response From District Officials

Sodus Central School District
P.O. Box 220
Sodus, New York 14551-0220
www.soduscsd.org
"Learning, Advancing, Proud, Spartans!"

District Office
(315) 483-4755 - fax

Nelson Kise
Superintendent
(315) 483-5201 - phone

Heather Uetz, Ed.D
Assistant Superintendent for Curriculum & Instruction
(315) 483-5234 - phone

Steven K. Moore
Business Administrator
(315) 483-5283 - phone

Joseph Keeney
Director of Student Services
(315) 483-5208 - phone
(315) 483-5248 - fax

Jr/Sr High School
(315) 483-6168 - fax

Arkee Allen
Principal
(315) 483-5280 - phone

Tina Peets, Ed.D
Assistant Principal
(315) 483-5261 - phone

Tim Padden
Director of Personalized Learning and Innovative Technology
(315) 483-5269 – phone

Intermediate School
(315) 483-5291 - fax

Gene Hoskins
Principal
(315) 483-5242 - phone

Elementary School
(315) 483-5292 – fax

Michael Sereno
Principal
(315) 483-5282 - phone

Transportation Office
(315) 483-5290 - fax

Jeremy Bricks
Transportation Supervisor
(315) 483-5273

November 10, 2022

[redacted] MBA
Office of the State Comptroller
The Powers Building
16 Wes Main Street – Suite 522
Rochester, NY 14614

Dear [redacted]

The Sodus Central School District would like to thank the auditors from the New York State Comptroller office for the comprehensive review of the Sodus Technology Department. Through the audit process five areas were identified as in need of correction. The Sodus Central School District wants to ensure that our network security is as protected as possible and accepts the findings of the audit. Please reference the Corrective Action Plan as to the steps that will be taken to remedy each of the five deficiencies.

At their November 10, 2022, meeting the Board of Education approved this Corrective Action Plan.

Sincerely,

[redacted]
Nelson Kise
Superintendent of Schools

[redacted]
Jason Walters
Board President

Cc: Tim Padden, Director of Personalized Learning and Innovative Technology
Matthew Wilbur, AV Telecommunications Technician and Technology Coordinator

Nurtured by the influence of a diverse community, our district is committed to the success of every student. We will support our students in developing the skills and strategies needed to achieve academic excellence and to become respectful, responsible, kind citizens of a global society. We are dedicated to sustaining an environment that fosters a joy for life and continued learning.

Sodus Central School District
P.O. Box 220
Sodus, New York 14551-0220

TO: Board of Education

FROM: Nelson Kise, Superintendent of Schools

DATE: October 24, 2022

RE: Approval of the Corrective Action Plan (CAP) for the Comptroller's Software Management Audit Report of Examination for Period Covered July 1, 2020-February 1, 2022

RESOLUTION

Resolved, that upon the recommendation of the Superintendent of Schools, the Board of Education of the Sodus Central School District, hereby approves the Corrective Action Plan for the Comptroller's Software Management Audit Report of Examination for period covered July 1, 2020-February 1, 2022.

CORRECTIVE ACTION PLAN – SODUS CSD COMPTROLLER AUDIT

COMMENT	ACTION	COMPLETION DATE	PERSON RESPONSIBLE
1. Maintain a complete and comprehensive software inventory list of all authorized, appropriate and necessary software applications installed on District computers.	All software, regardless of Ed Law 2D Part 121 compliance requirements, will be inventoried and revised throughout the school year on a regular basis. This will be cataloged in a spreadsheet within the IT department. As new software is adopted the list will be updated.	The initial list will be completed by December 1st, 2022. The list will be routinely updated.	Tim Padden and Matt Wilbur
2. Regularly examine computers, review software installations and uninstall any inappropriate, unnecessary and unauthorized software.	The Technology department will develop a schedule for routine maintenance and computer examination that will work in conjunction with school holidays, specifically the winter recess and summer recess. This will limit classroom instruction disruptions as students and staff will not be in school during these times.	This will be implemented starting with the 2022 winter recess and will be ongoing.	Matt Wilbur will schedule this routine with the BOCES IT Techs to ensure proper review of the computers.
3. Establish comprehensive written policies and procedures for reviewing software on District computers and monitoring software licenses.	The Sodus technology department will work with WFL BOCES to establish a written policy that meets the Districts needs regarding future software purchases and licensing. This will help ensure that proper software is installed that meets security requirements.	This will be completed by July 1st 2023.	Tim Padden and Matt Wilbur

CORRECTIVE ACTION PLAN – SODUS CSD COMPTROLLER AUDIT

4. Limit permissions for installing software to users who need these permissions to perform their job duties and responsibilities.	Administrative rights have been removed from all district-owned devices. Only Sodus IT department staff have administrative rights and will conduct all needed downloads on district-owned devices.	This is already completed and will continue on an as needed basis.	Matt Wilbur will coordinate any updates and downloads with BOCES IT Techs.
5. Ensure all users agree to the AUP's terms in writing.	A written Acceptable Use Policy will be drafted and shared with all staff for signature. This will be kept on record as part of the staff personnel file. The AUP will become part of the new hire process and be completed prior to the employee's start date.	This will be completed by January 1st, 2023.	Tim Padden and Matt Wilbur

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 relevant policies and procedures and interviewed District officials and employees to gain an understanding of IT and software management processes.
- We used our professional judgment to review 65 computers assigned to 34 employees. We determined our sample primarily based on risk related to information access and permissions on the District's network. We selected 100 percent of IT staff and approximately 50 percent of staff in the following categories: business office, administrators and special education. We reviewed all computers assigned to these users. We also randomly selected nine additional computers assigned to other District employees. We chose this random sample by assigning each computer a random number using Excel's Rand() function and selecting the first nine computers. In addition, we reviewed four other computers that did not have a specific user and that were located in the District's common areas.
- On December 7, 8 and 22, 2021, we ran a computerized audit script on the 65 computers in our sample to identify information pertaining to installed software, associated network user accounts with local administrative access to the computers and local user accounts.
- We compared software installed on the 65 computers in our sample with the District's software inventory list and discussed the software identified on the computers with IT staff to determine whether the software was authorized, appropriate and necessary.

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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