REPORT OF EXAMINATION | 2021M-83

Cornwall Central School District

Information Technology

AUGUST 2021

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

Contents

Report Highlights

Cornwall Central School District

Audit Objective

Determine whether Cornwall Central School District (District) officials established adequate internal controls over the District's user accounts and software updates to help prevent unauthorized use, access and loss.

Key Findings

District officials did not establish adequate internal controls to safeguard the District's user accounts. Specifically:

- Network user accounts were not adequately managed.
- Officials did not monitor compliance with the District's Acceptable Use Policy (AUP).
- The Board did not adopt adequate information technology (IT) policies or a disaster recovery plan.

Sensitive IT control weaknesses, including issues related to software updates, were communicated confidentially to officials.

Key Recommendations

- Develop written procedures for managing system access that include periodically reviewing user access and disabling unnecessary network user accounts.
- Monitor Internet use to ensure employees comply with the AUP.
- Adopt comprehensive IT policies and a disaster recovery plan.

District officials generally agreed with our findings and indicated they plan to initiate corrective action.

Background

The District is located in Orange County, New York. It includes the Village of Cornwall-on-Hudson, the Town of Cornwall, and portions of the Towns of New Windsor and Woodbury.The District has three elementary schools, one middle school and a high school.

The District is governed by a Board of Education (Board), which is composed of nine elected members who serve three-year terms. The Board is responsible for the general supervision of the District through setting policy and Board goals. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for the day-to-day management. The Director of Technology is responsible for all the District's IT functions and manages all IT infrastructure.

Quick Facts	
Students 2020-21	3,151
Employees (Full- and Part-Time)	471
Total Enabled Network User Accounts	3,904

Audit Period

July 1, 2019 – July 9, 2020

Information Technology

The District's IT system and data are valuable resources. The District relies on its IT assets for Internet access, email, and for maintenance of financial and personnel records, much of which contain personal, private and sensitive information (PPSI). If the IT system is compromised, the results could be catastrophic and 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.

We found unneeded network user accounts that District officials had not disabled or monitored.

Why Should District Officials Monitor Network User Accounts and Permissions?

User accounts provide users with access to the resources on a district's network and users computer 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 and view PPSI on the network. A district should have a written policy and procedures for granting, changing and revoking access rights to the 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 accounts as soon as there is no longer a need for them.

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 processes, 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. In addition, when multiple users are allowed to share network user accounts, there is no individual accountability should that account be used to violate policy or commit an electronic crime.

District Officials Did Not Adequately Manage Network User Accounts and Permissions

District officials did not establish procedures to manage network user accounts or maintain a current list of authorized network users and their level of access. We examined all 3,904 network user accounts to determine whether any were unneeded or had unneeded administrative permissions. We found unneeded network user accounts that District officials had not disabled or monitored.

- We identified 14 unnecessary user accounts that were not disabled or removed. Four retired employees and 10 resigned employees were still active in the system.

- We also reviewed all 185 generic accounts and found 140 generic accounts that were originally created for various uses and were no longer needed or had not been used in at least six months.
- We tested five computers for user permissions and found two users had unnecessary network and local administrative permissions.

The Assistant Superintendent for Business told us that the previous Director of Technology also served as the District's Data Coordinator and focused on reporting data to both the New York State Education Department and internally. He also said that the District's internal IT assessment, completed in May 2020, recommended to have a separate Director of Technology due to the District's size. As a result, in September 2020, the District hired a new Director of Technology, who is now making improvements to the IT systems at all levels.

If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. Because generic accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user.

[The District's] policy states that users shall not use system resources for non-instructional purposes…

How Should Officials Monitor Compliance with the AUP?

An AUP describes what constitutes appropriate and inappropriate use of IT resources, along with district management's expectations concerning personal use of IT equipment, and user privacy and consequences for violating the AUP.

The District has a comprehensive AUP that defines the procedures for computer, Internet and email use. The policy describes what constitutes appropriate and inappropriate use of IT resources and states that the Internet is to be used exclusively for instructional, research and administrative purposes. Specifically, the policy states that users shall not use system resources for non-instructional purposes including, but not limited to, personal email account access (e.g., Hotmail, AOL, Yahoo, Gmail, etc.), personal instant messaging (chatting), accessing social networking sites (e.g., Facebook, MySpace, Twitter, etc.), online shopping, online gaming or personal use of streaming media such as online radio stations, music videos or video broadcasts, accessing personal pictures/videos, unauthorized music access, unauthorized software installation/access, etc.

Monitoring compliance with AUPs involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity, and investigating and reporting such activity. 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. 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.

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 by configuring web filtering software to block access to unacceptable websites and limit access to sites that comply with a district's AUP.

Officials Did Not Monitor Compliance with the AUP

District officials and direct supervisors did not monitor employee Internet use or implement procedures to monitor for compliance with the District's AUP.

We reviewed the web browsing history on six computers used by District employees whose job duties routinely involved accessing PPSI. We found that two of these computers had questionable Internet use for personal email, online shopping, music radio stations and non-work-related web searching (Figure 1).

Figure 1: Questionable Internet Use

Type	Website
Job Search	Indeed.com, thebalancecareers.com
Entertainment	Christmas Music, YouTube, SiruisXM Radio, Z-100, Netflix.com
Shopping	amazon.com, lowes.com, lakeside.com, personalizationmall.com, enews.giftsforyounow.com
Personal Email	yahoo.com, gmail.com
Personal Online Banking	Walden Savings Bank

After we brought this to District officials' attention, the Director of Technology informed us that the District stopped all shopping websites through the filter. Because District officials did not monitor employee Internet use, they were unaware of this personal and inappropriate computer use.

When employees access websites for non-business or non-instructional purposes through the network, in violation of the District's AUP, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections (malware).

How Should IT Systems Be Secured and Protected?

IT policies such as a password security policy and wireless security policy describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board should establish security policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies. District officials should develop and communicate written procedures for storing, classifying, accessing and disposing PPSI. This policy should define PPSI; explain the entity's reasons for collecting PPSI; and describe specific procedures for the use of, access to, and storage and disposal of PPSI involved in normal business activities.

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event that compromises the availability or integrity of an IT system and data.

To minimize the risk of data loss or suffering a serious interruption of services, district officials should establish a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and availability or integrity of the district's IT system and data, including software applications and any PPSI contained therein. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities.

The Board Did Not Adopt IT Policies

The District does not have the following policies that describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations:

- PPSI protection policy to explain the reason for collecting PPSI. The District also does not have written procedures for use of, access to, and storage and disposal of PPSI involved in normal business activities.
- Password security policy and wireless security policy to describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations.
- Disaster recovery plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster or a phishing or ransomware attack, staff had no guidance or plan to follow to restore or resume essential operations in a timely manner.

District officials informed us that the Board had not developed these policies yet. Without a PPSI protection policy, there is an increased risk that PPSI could be exposed to unauthorized users, and effort to properly notify affected parties in the event of a data breach could be hampered. A lack of appropriate password security and wireless security policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Without a formal written disaster recovery plan, the District has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies to address PPSI protection, password security and wireless security to communicate to District officials and employees.

District officials should:

2. Maintain a list of authorized network users and routinely evaluate and disable any unnecessary accounts.
3. Monitor computer Internet use to ensure employees comply with the AUP.
4. Develop and test a comprehensive disaster recovery plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure it works as intended.

Appendix A: Response From District Officials

Cornwall Central School District

Terry J. Dade
Superintendent of Schools

Harvey Sotland
Assistant Superintendent for Business

Megan Argenio
Assistant Superintendent for Instruction

July 28, 2021

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

Dear Ms. Reynolds:

The Cornwall Central School District has received your draft report "Information Technology – Report of Examination – 2021M-083," which was reviewed and discussed at an exit conference with your staff on July 21, 2021. The District acknowledges and agrees with the findings and recommendations. With corrective measures already being initiated, a formal Corrective Action Plan (CAP) is being prepared and will be provided to the Comptroller's Office and the NYS Education Department.

We appreciate the time and effort undertaken by the Comptroller's Office and would like to thank your staff for doing so in a professional and courteous manner.

Sincerely,

Terry J. Dade
Superintendent of Schools

CC: Cornwall Central School District Board of Education
Harvey Sotland, Assistant Superintendent for Business

Central Administration, 24 Idlewild Avenue, Cornwall-on-Hudson, NY 12520 Phone: 845.534.8009 Fax 845.534.9032
www.cornwallschools.com

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 over the IT system and applications.
- We used our professional judgment to select a sample of six computers from the District's 1,223 computers. We reviewed web history reports from these computers to evaluate whether Internet use was in compliance with the acceptable use policy. We reviewed web history reports for accessed websites that could put the network at risk.
- We ran a computerized audit script to examine the District's domain controller. We then analyzed the report by comparing user accounts to a list of current employees to determine whether any network users were no longer employed by the District.
- We reviewed all 185 generic accounts that were originally created for various uses to determine whether they were still being used.

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 GAGAS (generally accepted government auditing standards). 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.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

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, Sullivan, Ulster, Westchester counties

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