THOMAS P. DiNAPOLI
COMPTROLLER

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER
110 STATE STREET
ALBANY, NEW YORK 12236

ROBIN L. LOIS, CPA
DEPUTY COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY
Tel: (518) 474-4037 Fax: (518) 486-6479

December 2025

Dr. Larry Dake, Superintendent
Members of the Board of Education
Chenango Valley Central School District
221 Chenango Bridge Road
Binghamton, NY 13901

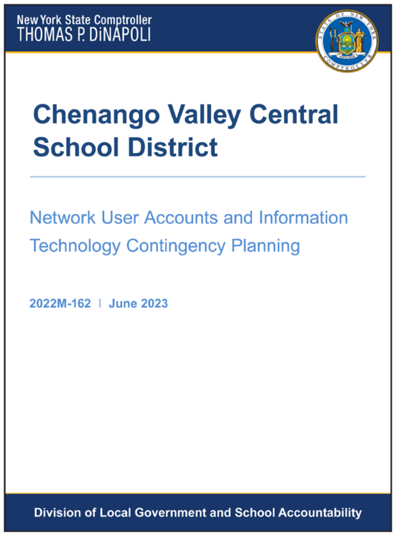
Report Number: 2022M-162-F

Dear Superintendent Dake and Members of the Board of Education:

One of the Office of the State Comptroller's (OSC) primary objectives is to identify areas where school district officials can improve their operations and provide guidance and services that will assist them in making those improvements. OSC also works to develop and promote short-term and long-term strategies to enable and encourage officials to reduce costs, improve service delivery and to account for and protect their assets.

In accordance with these objectives, we conducted an audit of the Chenango Valley Central School District (District) to determine whether District officials adequately managed nonstudent network user accounts and developed and adopted an information technology (IT) contingency plan. As a result of the audit, we issued a report, dated June 2023, identifying certain conditions and opportunities for the District IT Director's, Board of Education's (Board) and officials' review and consideration (Figure 1). In response to the audit, District officials filed a corrective action plan (CAP) with OSC on October 2, 2023.[1] The CAP identified the actions officials took or planned to take to implement the audit recommendations.

Figure 1: Chenango Valley Central School District 2023 OSC Audit Report



New York State Comptroller
THOMAS P. DiNAPOLI

Chenango Valley Central School District

Network User Accounts and Information Technology Contingency Planning

2022M-162 | June 2023

Division of Local Government and School Accountability

https://www.osc.ny.gov/files/local-government/audits/2023/pdf/chenango-valley-central-school-district-2022-162.pdf

To further our policy of providing assistance to local governments and school districts, we revisited the District in November 2025 to review progress in implementing the audit's recommendations. The follow-up review was limited to interviews with the District's Director of Technology (IT Director), other District personnel, and South Central Regional Information Center (SCRIC)

[1] See Appendix A for the District's CAP to the OSC audit report.

personnel and inspection of certain data and documents related to the issues identified in the report and confidential communications with District officials.[2]

Of the three recommendations contained in the 2022M-162 report, we determined, based on our limited procedures, that the District's IT Director, Board and officials fully implemented one recommendation and partially implemented two recommendations. As a result, the District's personal, private and sensitive information (PPSI)[3] and IT resources continued to have an increased risk for inappropriate access and compromise. We also reviewed progress in implementing the recommendations related to the sensitive IT control weaknesses that were reported to officials confidentially and communicated those results confidentially to District officials.

Recommendation 1 – Evaluate and Disable Unneeded Network User Accounts

The IT Director should evaluate all enabled network user accounts and disable any deemed unneeded.

Status of Corrective Action: Partially Implemented

Observations/Findings: The IT Director told us she conducts quarterly network user account reviews by cross-referencing a list of active employees against a list of enabled network user accounts received from the District's IT service provider, the SCRIC. We obtained and reviewed evidence related to the IT Director's three most recent reviews and confirmed they were performed quarterly as she asserted.

We also obtained and reviewed a list of enabled nonstudent network user accounts and determined all 68 network user accounts identified as unnecessary during the 2023 OSC audit were disabled as of November 2025. However, we determined during our review that nine of the 585 enabled nonstudent network user accounts were unnecessary as of November 2025, and District officials should have disabled them.

The IT Director told us that she had identified three of the nine unnecessary network user accounts in her most recent quarterly review, was aware that the three accounts' users had left District employment, and that she had a plan to disable the accounts after our testing was complete. The IT Director also told us she was unsure whether she should have received employee exit forms to request the remaining six unnecessary accounts be disabled upon the users leaving District employment, or whether the accounts belonged to substitute teachers still with the District. Upon our inquiry, the IT Director told us she planned to request the accounts be disabled and to continue working with District officials towards establishing effective procedures for managing the network user accounts within their computing environment.

[2] The audit also examined the adequacy of certain sensitive IT controls. Because of the sensitivity of some of this information, we communicated it confidentially to District officials.

[3] 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.

Until the IT Director ensures all unneeded network user accounts are disabled in a timely manner, additional entry points into the network will remain and the District's PPSI and IT resources continue to have an increased risk for inappropriate access and compromise.

Recommendation 2 – Develop and Monitor Network User Account Procedures

The IT Director should develop and monitor compliance with written procedures for granting, modifying and disabling user account access to the network and computers and for periodically reviewing user accounts and ensuring that SCRIC staff immediately disable network user accounts when access is no longer needed.

Status of Corrective Action: Partially Implemented

Observations/Findings: The IT Director did not develop written procedures for granting, modifying or disabling network user account access.

We requested the District's network user account procedures and reviewed the provided Computer Usage Policy and employee exit checklist. According to the IT Director, the District requires:

- All employees to read the Computer Usage Policy and complete an acknowledgment form before they are granted computer system access, and
- Supervisors to complete and submit the exit checklist when employees leave District employment and for the IT Director to request SCRIC disable the network user account access.

The IT Director told us that the District does not generally modify network user accounts other than for work location updates and substitute aide-to-teacher role transitions; when changes are required, SCRIC staff implement the change upon receiving a request from the IT Director submitted through the ticketing system.

We confirmed that relevant staff were provided with instructions and copies of the required employee exit checklist form. However, the IT Director and District officials told us that, in addition to the exit forms, they also review Board meeting minutes and retirement paperwork to assist in determining when network user accounts should be disabled. Further, District officials told us when accounts requiring disabling are identified through these alternative means, they do not require supervisors to submit missing exit checklist forms prior to disabling separating employees' accounts.

We requested and reviewed a list of employees who separated from the District and copies of employee exit forms that were submitted between October 2023 and October 2025. Although none had network user accounts enabled as of November 2025, of the 26 employees in roles that had required network user account access and who separated from the District during that period, 18 employees (69 percent) did not have exit forms submitted.

As noted in Recommendation 1, the IT Director told us she conducts quarterly network user account reviews by cross-referencing a list of active employees against a list of enabled network user accounts received from SCRIC staff. The IT Director does not have access to manage or view network user account data. Rather, they rely on SCRIC staff, the SCRIC ticketing system and the lists provided during quarterly reviews to ensure accounts are disabled by SCRIC staff.

District officials we spoke to, including the Superintendent, Business Executive and the IT Director were unable to explain why there were no written procedures for network user account management but agreed that they should document all current processes, including the employee exit checklist, Board meeting minutes and quarterly network user account reviews. Without developing and monitoring compliance with written network user account access procedures, District officials cannot ensure that SCRIC staff immediately disable network user accounts when access is no longer needed, such as the nine unnecessary network user accounts noted in Recommendation 1.

Recommendation 3 – Written IT Contingency Plan

The Board and District officials should develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

Status of Corrective Action: Fully Implemented

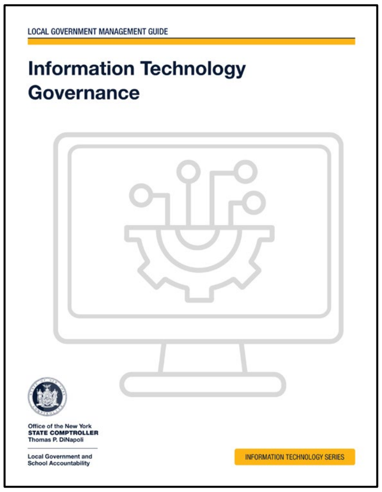
Observations/Findings: The IT Director developed a comprehensive IT contingency plan and the Board adopted the plan in November 2025. The plan describes the preparation and actions required to effectively respond to a disaster, assign responsibilities, develop strategies and specific procedures, conduct testing and after-action activities and update and maintain the plan. The IT Director told us, and we confirmed, that the District's IT contingency plan was distributed to all executive staff and necessary officials.

The IT Director also told us that the IT contingency plan will be included in the District's annual review of policies. In addition to the IT contingency plan, the IT Director developed an Incident Response Plan as set procedures used to locate and respond to cyber incidents within the District's information systems environment.

During our review, we discussed the basis for our recommendations and the operational considerations relating to these issues. We encourage the District's IT Director, Board and officials to continue their efforts to fully implement our recommended improvements. For additional guidance, the District's IT Director, Board and officials should refer to OSC's *Local Government Management Guides*: *Information Technology Governance, New York Local Government and School Cybersecurity: A Cyber Profile* and *Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders* which are available on our website (Figure 2).

Figure 2: OSC Publications

Information Technology Governance



LOCAL GOVERNMENT MANAGEMENT GUIDE

Information Technology Governance

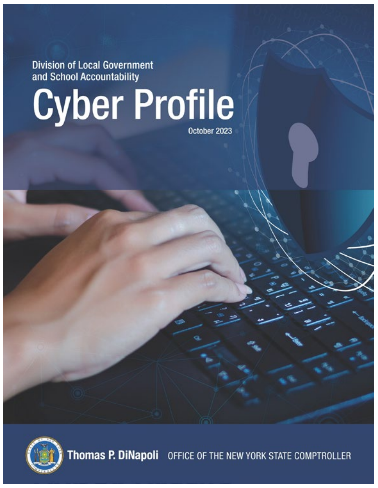
Office of the New York STATE COMPTROLLER Thomas P. DiNapoli

Local Government and School Accountability

INFORMATION TECHNOLOGY SERIES

https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf

New York Local Government and School Cybersecurity: A Cyber Profile



Division of Local Government and School Accountability

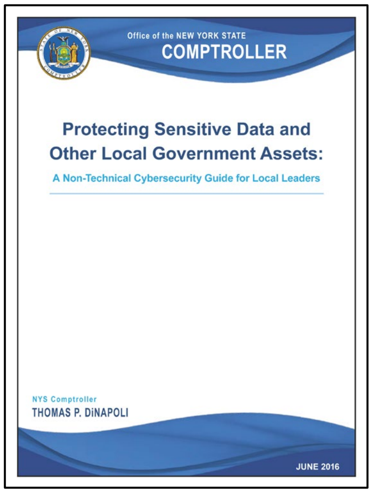
Cyber Profile

October 2023

Thomas P. DiNapoli OFFICE OF THE NEW YORK STATE COMPTROLLER

https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-school-cyber-profile.pdf

Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders



Office of the NEW YORK STATE COMPTROLLER

Protecting Sensitive Data and Other Local Government Assets:

A Non-Technical Cybersecurity Guide for Local Leaders

NYS Comptroller THOMAS P. DiNAPOLI

JUNE 2016

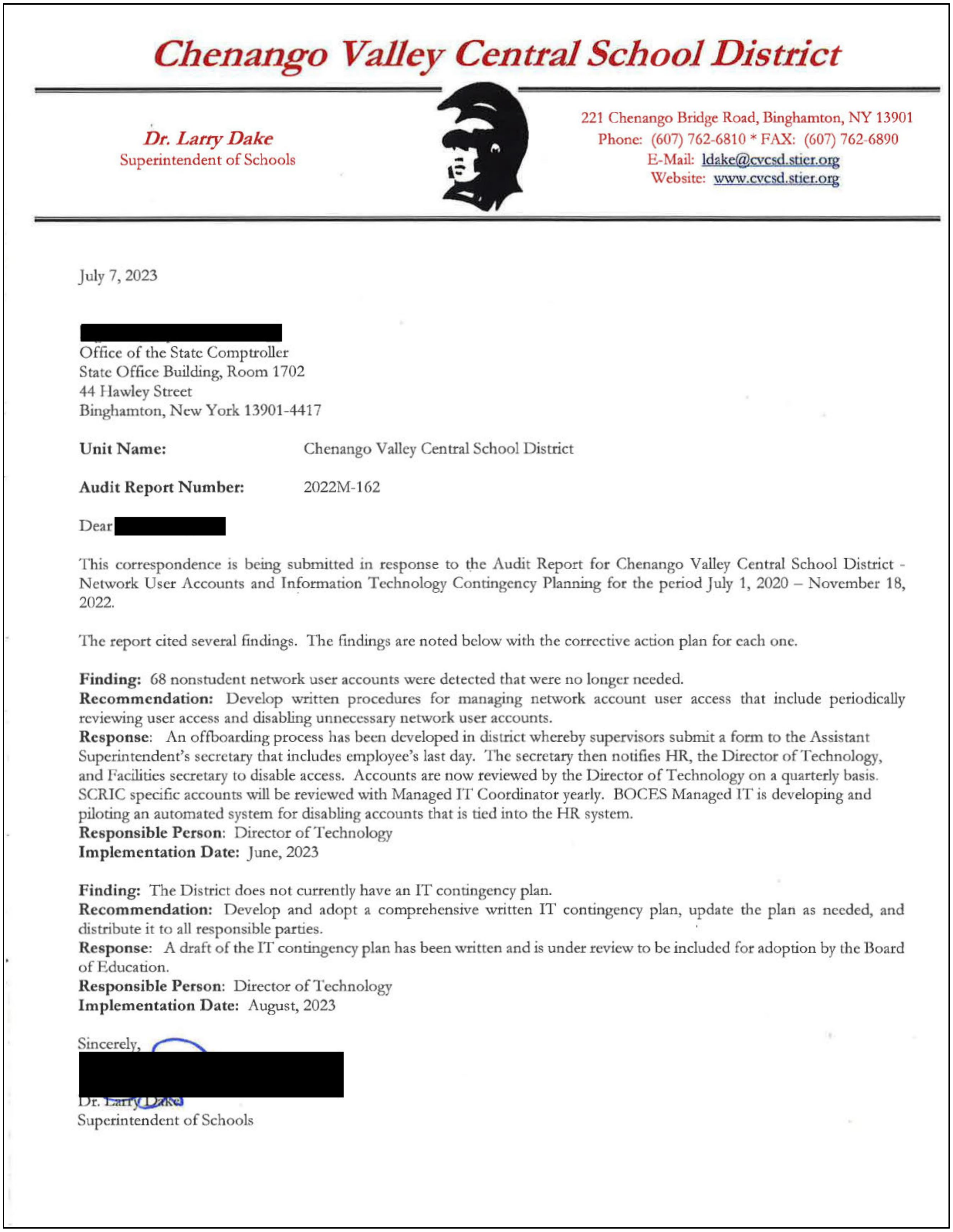
https://www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf

Thank you for the courtesies and cooperation extended to our auditors during this review. If you have any further questions, please contact Jennifer Kenneson, Chief Information Systems Auditor, at (518) 738-2639.

Sincerely,

Robin L. Lois, CPA
Deputy Comptroller

Appendix A – District's CAP for the OSC Audit Report



Chenango Valley Central School District

Dr. Larry Dake
Superintendent of Schools

221 Chenango Bridge Road, Binghamton, NY 13901
Phone: (607) 762-6810 * FAX: (607) 762-6890
E-Mail: ldake@cvcsd.stier.org
Website: www.cvcsd.stier.org

July 7, 2023

[redacted]
Office of the State Comptroller
State Office Building, Room 1702
44 Hawley Street
Binghamton, New York 13901-4417

Unit Name: Chenango Valley Central School District

Audit Report Number: 2022M-162

Dear [redacted]

This correspondence is being submitted in response to the Audit Report for Chenango Valley Central School District - Network User Accounts and Information Technology Contingency Planning for the period July 1, 2020 – November 18, 2022.

The report cited several findings. The findings are noted below with the corrective action plan for each one.

Finding: 68 nonstudent network user accounts were detected that were no longer needed.
Recommendation: Develop written procedures for managing network account user access that include periodically reviewing user access and disabling unnecessary network user accounts.
Response: An offboarding process has been developed in district whereby supervisors submit a form to the Assistant Superintendent's secretary that includes employee's last day. The secretary then notifies HR, the Director of Technology, and Facilities secretary to disable access. Accounts are now reviewed by the Director of Technology on a quarterly basis. SCRIC specific accounts will be reviewed with Managed IT Coordinator yearly. BOCES Managed IT is developing and piloting an automated system for disabling accounts that is tied into the HR system.
Responsible Person: Director of Technology
Implementation Date: June, 2023

Finding: The District does not currently have an IT contingency plan.
Recommendation: Develop and adopt a comprehensive written IT contingency plan, update the plan as needed, and distribute it to all responsible parties.
Response: A draft of the IT contingency plan has been written and is under review to be included for adoption by the Board of Education.
Responsible Person: Director of Technology
Implementation Date: August, 2023

Sincerely,

[redacted]

Superintendent of Schools