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

Contents

Report Highlights

Chenango Valley Central School District

Audit Objective

Determine whether Chenango Valley Central School District (District) officials adequately managed nonstudent network user accounts and developed and adopted an information technology (IT) contingency plan.

Key Findings

District officials did not adequately manage network user accounts or develop and adopt an IT contingency plan. In addition to finding sensitive IT control weaknesses, which we communicated confidentially to officials, we found that:

- Sixty-eight, or 12 percent, of the District's nonstudent network user accounts were no longer needed. Unneeded network user accounts are additional entry points into a network and, if accessed by attackers, could be used to inappropriately access and view personal, private and sensitive information (PPSI) or disable the network.
- Without an IT contingency plan, the District has an increased risk that it could suffer a serious interruption to operations since the District's ability to communicate during a disruption or disaster will affect the timely processing of its business functions.

Key Recommendations

- Develop written procedures for managing network account user access that include periodically reviewing user access and disabling unnecessary network user accounts.
- Develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

District officials agreed with our recommendations and indicated they will take and have taken corrective action.

Background

The District serves the Towns of Chenango, Colesville, Dickinson, Fenton and Kirkwood in Broome County.

The District is governed by an elected nine-member Board of Education (Board), responsible for managing and controlling financial and educational affairs.

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

The District contracts with the Broome-Delaware-Tioga Board of Cooperative Educational Services (BT BOCES) South Central Regional Information Center (SCRIC) to provide IT services. The District employs a full-time IT Director who acts as liaison between the District and SCRIC.

Quick Facts	
Nonstudent Network Accounts Reviewed	All 570
Full and Part-Time Employees	531
IT Service Contract for 2021-22	$1.5 million

Audit Period

July 1, 2020 – March 11, 2022.

We extended our audit period to November 18, 2022 to review updates to certain active user accounts

Network User Accounts and Information Technology Contingency Planning

School district officials are responsible for managing network user accounts, which provide access to network resources and data needed to complete job duties and responsibilities.

How Should District Officials Manage Nonstudent Network User Accounts?

School district officials should actively manage all district network user accounts including nonstudent network user accounts (e.g., staff, shared and service accounts,[1] third-party vendors). Network user account management includes their creation, use and dormancy, and regularly monitoring them to ensure they are appropriate and authorized. User accounts that are no longer needed should be disabled immediately. School district officials should adopt written procedures to help guide network and system administrators in properly granting, modifying and disabling user account access to school district networks. Also, these procedures should require school district officials to periodically review enabled user accounts to ensure they are appropriate and authorized.

District Officials Did Not Adequately Manage Network User Accounts

We identified 68 enabled network user accounts that were no longer necessary, as follows:

- 56 enabled network user accounts were assigned to former employees and substitutes. The IT Director told us that 26 of these accounts are assigned to former substitutes whose accounts remain enabled based on their active status per the District's approved substitute list for the upcoming school year, although they have not substituted during the audit period. The remaining 30 user accounts are former employees whose last paycheck was issued more than one year ago but were not disabled. We reviewed these 56 accounts with the IT Director and verified they were deleted after we brought it to the IT Director's attention, during our audit inquiry.
- Out of 16 enabled network user accounts that did not match an active District employee or SCRIC employee,[2] six user accounts were no longer needed. We verified that these six unneeded user accounts were subsequently deleted. According to the IT Director, the remaining 10 user accounts were necessary in order to delegate access rights to an application.

[1] Service accounts are not linked to individual users and may be needed for certain network services or applications to run properly. Shared accounts are accounts that are used by more than one user for the purpose of logging on to a computer system and accessing network resources. For example, service accounts can be created and used for automated back-ups, while shared accounts may be used for testing processes, training purposes or for shared email accounts, such as a service helpdesk account.

[2] These accounts included third-party users such as school resource officers; BT BOCES employees stationed at the District; sports team trainers; a Head Start teacher provided by Broome County; a heating, ventilation and air conditioning vendor; health educators and a special education service provider.

- Two shared accounts and two service accounts were no longer being used and should have been disabled. We shared our findings with the IT Director and verified that these four accounts were deleted.
- One user account was duplicated, and one user account was unknown to officials. The duplicated account was never used to log on to the network. There was no record available at the District for the unknown user, who last accessed the account over three years ago, but the account was assigned to the same organizational unit as substitute teachers, a lifeguard and a student employee. We reviewed documentation and verified that these two user accounts were deleted because District officials agreed with our inquiry.

While the District had a system to approve new nonstudent network accounts, change existing accounts and monitor for unnecessary accounts, this did not always occur. For example, the IT Director's annual review of enabled accounts did not sufficiently identify all accounts needing to be deleted.

Unneeded network user accounts are additional entry points into a network and, if accessed by attackers, could be used to inappropriately access and view personal, private and sensitive information (PPSI)[3] accessible by those accounts and potentially compromise IT resources.

Unneeded network user accounts are additional entry points into a network. …

Why Should District Officials Develop and Adopt a Comprehensive Written IT Contingency Plan?

To help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster, the board and district officials should develop and adopt a comprehensive written IT contingency plan. These events can include power outages, software or hardware failures caused by a virus or other type of malicious software (e.g., ransomware), human error, equipment destruction or a natural disaster (e.g., flood, fire). An IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to recover data and quickly resume operations in the event of an unplanned disruption. Additionally, IT contingency plans should include data back-up procedures, such as ensuring backups are stored off-site and off-network and requiring IT staff to periodically test backups to ensure they will function as expected.

School district officials should periodically test and update the plan, as needed, to help ensure officials understand their roles and responsibilities during and after a disruptive event. Testing and updating IT contingency plans are particularly

[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.

important given the ongoing and increasingly sophisticated threat of ransomware attacks. These plans should be distributed to key officials to help ensure they understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements.

District Officials Did Not Develop and Adopt a Comprehensive Written IT Contingency Plan

The Board and District officials did not develop and adopt an IT contingency plan to document and inform staff how they should respond to unplanned disruptions and disasters that affect the District's IT environment. The IT Director told us that she thought the previous IT Director had developed an IT contingency plan, but she was unable to locate it. Consequently, in the event of a disruption or disaster – including a ransomware attack or other unplanned event – District staff do not have sufficient documented guidance or plans to follow to recover data and resume essential operations in a timely manner and help minimize damage and recovery costs.

The Board contracted for select IT services, including nightly backups of all data, applications and operating systems. These daily backups were encrypted and stored at a secure, off-site location. According to the IT Director, backups were periodically restored, and the most recent restoration was successful. We examined documentation supporting the successful restoration of a deleted folder from its backup on this date.

The IT Director told us that an IT committee is currently working on developing a written IT contingency plan as a result of our audit, and the IT Director provided us with a draft of this policy. However, in the event of disruption or disaster, the IT Director told us that the District would rely on their contractor to return the District to service, in conjunction with a likelihood to borrow necessary equipment from neighboring districts.

While the IT Director did provide ideas for the District's likely response to unplanned cyber events, without a formal and comprehensive IT contingency plan, the District has an increased risk that it could suffer a serious interruption to operations since the District's ability to communicate during a disruption or disaster will affect the timely processing of its business functions.

What Do We Recommend?

The IT Director should:

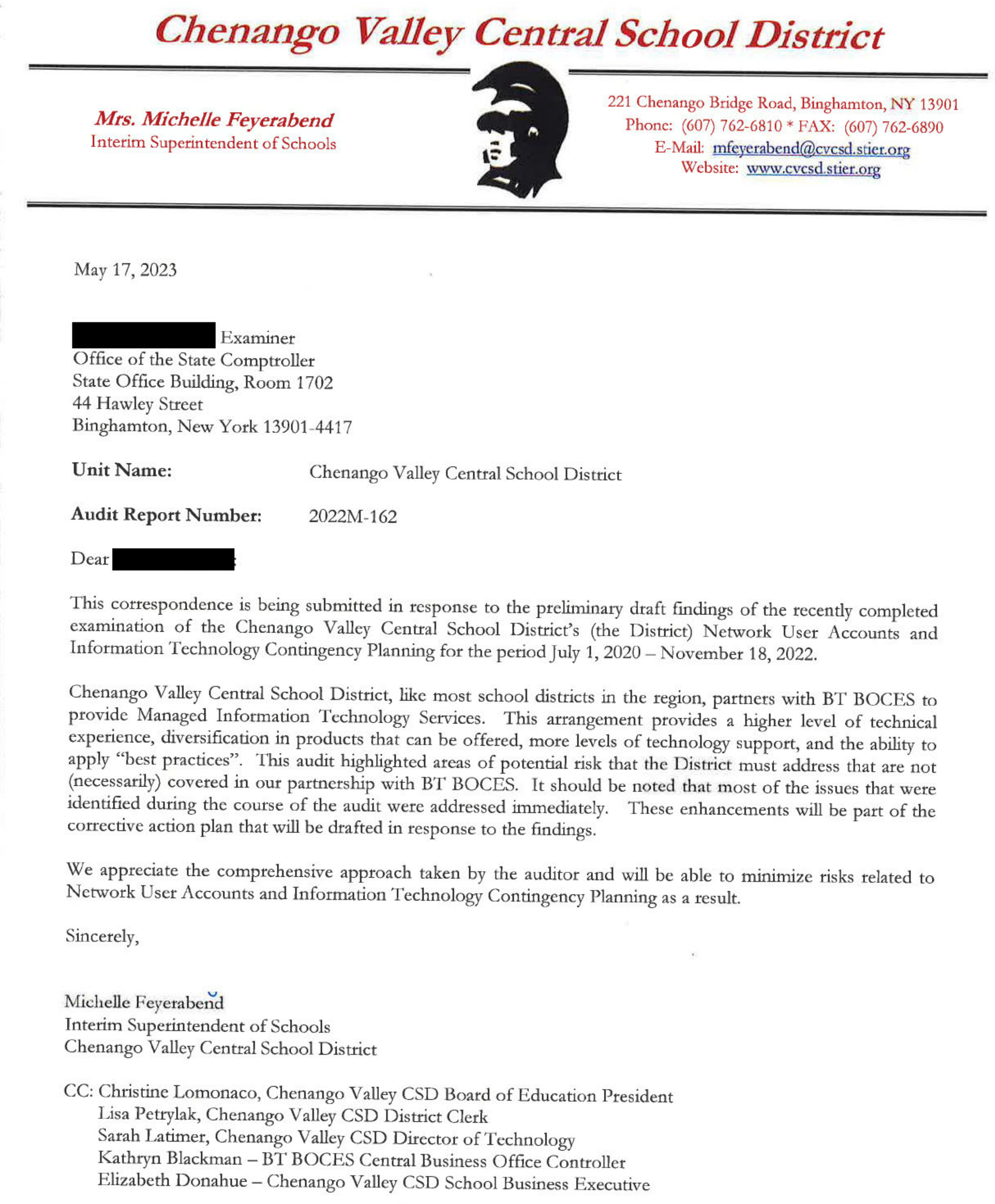
1. Evaluate all enabled network user accounts and disable any deemed unneeded.

2. 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.

The Board and District officials should:

3. Develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

Appendix A: Response From District Officials



Chenango Valley Central School District

Mrs. Michelle Feyerabend
Interim Superintendent of Schools

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

May 17, 2023

[redacted] Examiner
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 preliminary draft findings of the recently completed examination of the Chenango Valley Central School District's (the District) Network User Accounts and Information Technology Contingency Planning for the period July 1, 2020 – November 18, 2022.

Chenango Valley Central School District, like most school districts in the region, partners with BT BOCES to provide Managed Information Technology Services. This arrangement provides a higher level of technical experience, diversification in products that can be offered, more levels of technology support, and the ability to apply "best practices". This audit highlighted areas of potential risk that the District must address that are not (necessarily) covered in our partnership with BT BOCES. It should be noted that most of the issues that were identified during the course of the audit were addressed immediately. These enhancements will be part of the corrective action plan that will be drafted in response to the findings.

We appreciate the comprehensive approach taken by the auditor and will be able to minimize risks related to Network User Accounts and Information Technology Contingency Planning as a result.

Sincerely,

Michelle Feyerabend
Interim Superintendent of Schools
Chenango Valley Central School District

CC: Christine Lomonaco, Chenango Valley CSD Board of Education President
Lisa Petrylak, Chenango Valley CSD District Clerk
Sarah Latimer, Chenango Valley CSD Director of Technology
Kathryn Blackman – BT BOCES Central Business Office Controller
Elizabeth Donahue – Chenango Valley CSD School Business Executive

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 SCRIC staff and reviewed Board meeting minutes and District and SCRIC IT policies and procedures to gain an understanding of the District's IT operations, including management of nonstudent network user accounts and whether the District has an IT contingency plan. We reviewed confirmation regarding a deleted network folder to ensure that the folder was successfully restored from a backup.
- We ran a computerized audit script on the District's network on March 9, 2022. We then analyzed each report generated by the script, looking for weaknesses in network user account management. We reviewed all 570 nonstudent network user accounts and compared them to current employee and SCRIC employee lists to identify unused and other possibly unneeded network user accounts and permissions.

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.

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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief of Municipal Audits

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins counties