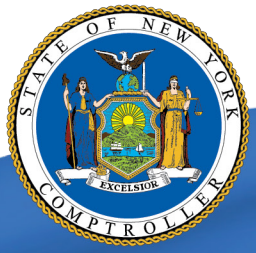
REPORT OF EXAMINATION | 2021M-155

Spencer-Van Etten Central School District

Information Technology

DECEMBER 2021



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

Contents

Report Highlights

Spencer-Van Etten Central School District

Audit Objective

Determine whether the Spencer-Van Etten Central School District (District) officials ensured District computerized data was safeguarded.

Audit Results

District officials have generally taken adequate steps towards helping to ensure computerized data was safeguarded through managing user accounts, providing adequate training and adopting and distributing a written information technology (IT) contingency plan.

However, certain sensitive IT control weaknesses and audit recommendations were communicated confidentially to officials.

District officials agreed with our audit results.

Background

The District serves the Towns of Baldwin, Chemung, Erin and Van Etten in Chemung County, the Towns of Spencer, Barton and Tioga in Tioga County, the Towns of Danby and Newfield in Tompkins County and the Town of Cayuta in Schuyler County.

The District is governed by a seven-member Board of Education (Board) which is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer and is responsible for the day-to-day management, under the direction of the Board.

The District contracts with the Greater Southern Tier (GST) Board of Cooperative Educational Services (BOCES) to provide IT services and is a member of the GST BOCES regional IT network. BOCES staff adds, deletes and modifies user accounts at the District's direction.

Quick Facts	
Number of Nonstudent Accounts	236
Number of Student Accounts	800
Number of Employees	264

Audit Period

July 1, 2019 – March 2, 2021

Information Technology

Why Should District Officials Manage User Accounts?

Network user accounts provide access to school district network resources and should be actively managed to safeguard computerized data. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI),[1] make changes to employee or student records or deny access to computerized data.

To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer used or needed, they should be disabled in a timely manner. A school district should have written policies and procedures for granting, changing and removing user access and permissions to the network.

To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions. …

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. School districts should limit the number of shared generic user accounts. 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 and disable any generic accounts that are not related to a specific need. A local user account is an account created to allow users to access resources on specific computers. These accounts are managed individually on each computer.

Officials Generally Managed User Accounts Properly

The District adopted a written data network and security policy that provides for managing user accounts and permissions. The policy requires officials to periodically grant, change and terminate user access rights to the District's computer systems and applications and ensures that users are given access based on, and necessary for, their job duties. Officials have procedures that include disabling user accounts once an employee leaves the District and deleting the account 30 days later. The District's policy also requires officials to annually review a report of all user accounts assigned access to the District IT system and make updates as needed.

1 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.

Nonstudent network user accounts represent user accounts assigned to employees, accounts shared by specific employee groups and generic accounts used by BOCES staff for administrative purposes. We reviewed all 236 nonstudent network user accounts, including 29 generic accounts, and all four local user accounts enabled on two users' computers, to determine whether the accounts were actively managed and found two minor exceptions which were discussed with District officials.

Why Should Officials Provide IT Security Awareness Training to Employees?

Officials should ensure computer users are aware of security risks and trained in practices that reduce internal and external threats to IT systems and safeguard data from potential abuse or loss. While IT policies define District officials' expectations and tell computer users what to do, IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on but is not limited to:

- Emerging trends in information theft and other social engineering reminders.
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed.
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet.
- Password controls.
- The restriction of physical access to IT systems and resources and how to protect them from intentional or unintentional harm, loss or compromise.

Officials Provided IT Security Awareness Training to Employees

The Board adopted administrative procedures requiring employees to be trained in the proper usage of the IT infrastructure, software and data. Officials provided employees with annual IT security awareness training to help ensure they understood IT security measures designed to safeguard data from potential abuse or loss. In addition to the annual training, employees received weekly email newsletters which contained useful IT tips and best practices that they can implement in their daily activities including:

- Identifying unexpected, suspicious notifications and identifying illegitimate websites.
- Identifying vendor impersonation, gift card fraud, stolen direct deposits and medical identity theft.

- Creating adequate passwords and security pins.
- Guidance on how to avoid accounts being compromised.

We reviewed the mandatory training materials and found that the materials adequately addressed emerging trends that could compromise PPSI and data. District officials implemented procedures to ensure that all employees completed the training. We also found that generally, employees accessed the weekly tips.

Why Should a District Develop an Information Technology Contingency Plan?

To minimize the risk of data loss or suffering a serious interruption of service, school district officials should establish a comprehensive written IT contingency plan. The plan should address the potential for sudden, unplanned disruptions (e.g., ransomware or other malware attack, inadvertent employee action or fire) that could compromise the network and the availability or integrity of the school district's IT system and data, including its applications and PPSI.

Typically, an IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to maintain or quickly resume operations. It should also reference how the school district should back up its computer systems. Backup data should be stored at a secure offsite location, maintained off-network, encrypted and routinely tested to ensure its integrity. The plan should be periodically tested, shared and updated to ensure key officials understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements.

Officials Developed and Distributed an Information Technology Contingency Plan

Officials have developed and distributed a written IT contingency plan to appropriate District officials. The District's data is backed up regularly, encrypted and stored in several secure and restricted offsite facilities. BOCES officials are responsible for continually testing parts of the regional network to ensure strategies are in place for quick recovery of its key business processes. For example, they test education and reporting applications maintained by BOCES and used by District staff and students, security, phone and the financial system, and are continually adding redundancy to the network. This redundancy helps to keep the regional network running in the event of an unplanned IT disruption so that the District can function. As part of the IT services provided by BOCES, a regional disaster recovery team holds regular meetings to review, discuss and update the contingency plan based on different IT disruption scenarios. BOCES staff assigned onsite at the District told us that they have successfully tested backups to ensure the data's integrity.

The District's data is backed up regularly, encrypted and stored in several secure and restricted offsite facilities.

Conclusion

District officials have generally taken adequate steps towards helping to ensure computerized data was safeguarded through managing user accounts, providing adequate training and adopting and distributing an IT contingency plan.

Appendix A: Response From District Officials

Spencer-Van Etten Central School
District Office
16 Dartts Crossroad
Spencer, New York 14883
(607) 589-7100
FAX (607) 589-3010

Ms. Diahann Hesler
Superintendent of Schools

December 1, 2021

Office of the State Comptroller
Anne Singer, Chief Examiner
State Office Building, Room 1702
44 Howley Street
Binghamton, NY 13901

RE: NYSOSC Audit Report Number 2021M-155, Information Technology

Dear Ms. Singer:

This letter is intended to acknowledge the draft copy of the New York State Comptroller's audit on the districts' information technology practices and procedures for the audit period of July 1, 2019 – March 2, 2021.

The Spencer-Van Etten Board of Education and the current administration strive to safeguard network infrastructure of the district. The districts' information technology team works collaboratively with the Greater Southern Tier BOCES regional information center to manage our systems to ensure proper management of the network.

Thank you to you and your team as we worked to complete a successful audit.

Sincerely,

Diahann Hesler
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 Board's adopted policies and procedures, the District's written IT contingency plan and meeting minutes, and interviewed District and GST BOCES staff to gain an understanding of the District's IT environment and internal controls to determine whether the policies and procedures in place were adequate.
- We reviewed available documentation to determine whether officials were monitoring and/or enforcing the Board adopted policies and procedures.
- We reviewed available documentation and made inquiries of District officials to determine whether IT security awareness training was provided to employees who use the District's IT resources and whether employees were reviewing weekly newsletters.
- We reviewed the District's network user accounts and related settings using a specialized audit script. We excluded student network accounts, as these accounts had more restricted access and are considered lower risk for potential access to computerized data containing PPSI. We reviewed the remaining 236 nonstudent network accounts and compared these accounts to the active employee list and payroll records and discussed these accounts with District officials to identify inactive and unused accounts.
- We reviewed a biased judgmental sample of two computers assigned to two employees (with four local accounts) due to potential access to PPSI and the level of access permissions granted to each user. We reviewed the local administrative access granted to these users against the users' job responsibilities and discussed with District officials to determine whether their access levels were appropriate for their job responsibilities.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss those audit results and recommendations 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.

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 Examiner

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, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins counties

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