REPORT OF EXAMINATION | 2019M-181

Newfield Central School District

Information Technology

DECEMBER 2019

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

Contents

Report Highlights

Newfield Central School District

Audit Objective

Determine whether the Board and District officials ensured District information technology (IT) assets and computerized data were safeguarded.

Key Findings

- District officials did not develop procedures for managing, limiting and monitoring user accounts and securing personal, private and sensitive information (PPSI).
- District officials generally maintained proper asset inventory records and provided IT security awareness training for District employees.

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

Key Recommendations

- Thoroughly review user accounts on a routine basis and disable any unnecessary network accounts as soon as they are no longer needed.

District officials agreed with our findings and recommendations and indicated they have taken, or planned to take, corrective action.

Background

The Newfield Central School District (District) serves six towns in Tompkins, Tioga and Chemung counties.

The District is governed by a seven-member Board of Education (Board) that is responsible for the general management and control of the District's financial and education affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for the District's administration.

The District employs a Director of Technology and Professional Development (Director) and two network specialists who provide IT support to District staff and students.

Quick Facts	
Desktop, Laptop and Tablet Computers	850
Total Network Accounts	1,152
Non-Student Network Accounts	395

Audit Period

July 1, 2017 – June 30, 2019

Information Technology

Why Should the District Manage User Accounts?

User accounts enable the IT system to recognize specific users and grant authorized permissions to users. However, user accounts are potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI). A district should have written procedures for granting, changing and revoking user permissions to the network.

In addition, to minimize the risk of unauthorized access, district officials should regularly review user accounts, including generic accounts,[1] to ensure they are still needed. Officials must disable unnecessary accounts as soon as there is no longer a need for them.

Officials Did Not Adequately Manage User Accounts

District officials did not develop procedures for managing, limiting and monitoring user accounts and permissions and securing PPSI. We reviewed all of the District's 395 non-student accounts[2] and found the following unnecessary accounts:

- 14 accounts (4 percent) had not been used in at least one year and were not associated with current employees. These accounts were for a former Board member, former employees, substitute teachers, and a parent-teacher association. We discussed these exceptions with one of the District's network specialists and determined that the accounts were not needed. He deleted these accounts while we were onsite.
- 65 accounts (16 percent) were generic accounts and had not been used in at least one year. The accounts were unneeded and a network specialist deleted or disabled these accounts while we were onsite.

Any unneeded network accounts should be disabled as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to access PPSI.

Why Should the District Maintain Accurate and Up-To-Date IT Asset Inventory Records?

Computer asset management is of particular importance to larger entities such as school districts that have many different users who perform a variety of

1 Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if necessary.

2 These included network accounts for 282 current and former District employees and independent contractors and 113 generic accounts.

functions. Maintaining complete and comprehensive inventory records is crucial in safeguarding IT assets from loss or theft. These inventory records should be checked and matched periodically with all district-owned computers to ensure that all IT assets are accounted for. Maintaining complete and up-to-date computer inventory records also helps the board develop and implement an effective technology replacement plan.

District Officials Generally Maintained Accurate and Up-To-Date IT Asset Inventory Records

The network specialists maintained a hardware inventory that included devices, model and serial numbers and inventory tag numbers, when applicable.

We matched all 106 serial numbers of computers purchased during the scope period to the District's inventory list, then selected 20 serial numbers from the inventory list and matched 19 of them to the physical asset. One tablet computer could not be located on campus. A network specialist told us this asset was damaged and disposed of, but could not produce documents supporting its disposal.

Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training that explains rules of behavior for using the Internet and IT systems and data, and communicates related policies and procedures to all employees and students. The training should center on emerging trends such as information theft and social engineering attacks,[3] computer viruses and other types of malicious software, all of which may result in PPSI compromise. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

3 Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

District Employees Were Provided With IT Security Awareness Training

The District provided users with IT security awareness training to help ensure they understood IT security measures. All faculty are required to take annual Internet browser and cybersecurity training that shows users safe browsing practices. The training is administered online and the Superintendent verifies that all users have completed the training.

We reviewed the training materials and found that the training adequately addressed emerging trends that could compromise PPSI and data. More specifically, it addressed web browser security, social engineering tactics, computer viruses, malicious software and proper password criteria.

What Do We Recommend?

District officials should ensure the Director:

1. Thoroughly reviews user accounts and permissions on a routine basis and disables any unnecessary network accounts as soon as they are no longer needed.
2. Maintains documentation of asset disposals.

Appendix A: Response From District Officials

December 13, 2019

Office of the State Comptroller
State Office Building Room 1702
44 Hawley Street
Binghamton, NY 13901-4417

To Whom It May Concern:

We have reviewed the Newfield Central School District Information Technology Report of Examination audit conducted by the Office of the State Comptroller. This letter is the official response of the Newfield Central School District to the audit findings.

The audit reported two key findings:

- District officials did not develop procedures for managing, limiting and monitoring user accounts and securing personal, private and sensitive information (PPSI).
- District officials generally maintained proper asset inventory records and provided IT security awareness training for District employees.

We are in agreement with these findings and appreciate the OSC's time and effort in helping to uncover any weaknesses in our IT procedures and for their suggestions for improvement.

Audit Recommendations were:

- Thoroughly review user accounts and permissions on a routine basis and disable any unnecessary network accounts as soon as they are no longer needed.
- Maintain documentation of asset disposals.

District Response:

- The District's Director of Technology & PD will review user accounts after resignations are approved by the Board of Education. In addition, a monthly review of accounts will help insure permissions and user accounts are all up-to-date and secure.
- The Technology Department will use the District's Disposal Forms for approval of all asset disposals and permanently maintain such records.
- The District plans to conduct an asset inventory project with OCM BOCES in the 2020-21 school year.

The District will continue to be proactive in implementing security measures for technology. For example, we have recently purchased data privacy and security services through OCM that will increase internet security and provide support for the District in this area.

Sincerely,

Dr. Cheryl Thomas, Superintendent

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 our audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of the District's IT operations and determine the adequacy of the policies and procedures.
- We compared serial numbers of all 106 computers purchased during the scope period to the District's inventory list to ensure all purchases were inventoried. We also selected a random sample of 20 serial numbers from the inventory list and traced them to the physical assets to ensure the IT assets were accounted for.
- We used our professional judgment to select all 395 non-student network accounts, based on their higher user permissions. We reviewed the last sign-on of the accounts, compared the accounts to the staff directory and discussed them with IT personnel to identify inactive and unnecessary accounts.

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 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.

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 District Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/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/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

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/localgov/index.htm

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, Sullivan, Tioga, Tompkins counties

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