REPORT OF EXAMINATION | 2022M-19

Franklin Central School District

Information Technology

JUNE 2022

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

Contents

Report Highlights

Franklin Central School District

Audit Objective

Determine whether Franklin Central School District (District) officials adequately managed network and local user accounts and software and developed an information technology (IT) contingency plan.

Key Findings

District officials did not adequately manage network user accounts, periodically compare installed software to an authorized software inventory or develop an IT contingency plan. In addition to finding sensitive information technology control weaknesses, which we communicated confidentially to officials, we found that:

- Nine of the District's network user accounts (8 percent) were not needed. This created additional network entry points that, if accessed by attackers, could be used to inappropriately access and view sensitive information and compromise IT resources.
- District staff did not have sufficient documented guidance or plans to follow to recover data and resume essential operations in a timely manner.

Key Recommendations

- Develop written procedures for managing computers and network user accounts.
- Periodically compare installed software to an authorized software inventory list.
- Develop and adopt a comprehensive written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The District serves the Towns of Davenport, Franklin, Meredith, Sidney and Walton in Delaware County and the Town of Otego in Otsego County.

The District is governed by an elected five-member Board of Education (Board) that is responsible for managing and controlling the District's 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.

The District's IT Department consists of a Network Manager/ District Data Coordinator (Network Manager) and a computer technician who manage the District's network and local user accounts, security settings and software.

Quick Facts	
Nonstudent Network Accounts Reviewed	109 (100 percent)
Local User Accounts Reviewed	7
Servers and Computers Reviewed	8
Employees	84

Audit Period

July 1, 2020 – November 5, 2021

Information Technology

The District's Business Manager is responsible for notifying the IT Department of necessary changes to user access rights. The District also contracts with the South Central Regional Information Center (SCRIC) to provide IT back-up services.

How Should Officials Manage Network and Local User Accounts?

School district officials are responsible for managing network and local user accounts, which provide access to network and computer resources and data needed to complete job duties and responsibilities. Because user accounts are potential entry points for attackers, school district officials should properly manage these accounts to help minimize the risk that they could be misused. If user accounts are compromised, they could be used to breach and/or compromise data stored on a school district's network or computers and/or could disrupt school district IT systems.

When user accounts are no longer needed, they should be disabled in a timely manner.

To minimize the risk of unauthorized access, school district officials should actively manage user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner. School district officials should adopt written procedures to help guide network and system administrators in properly granting, modifying and disabling user access to school district networks and computers. Also, these procedures should require school district officials to periodically review user accounts to ensure they are necessary.

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 back-up or testing processes, training purposes or generic email accounts, such as a service helpdesk account. School district officials should routinely evaluate generic network user accounts and disable those that are not related to a specific need.

Officials Did Not Adequately Manage Network User Accounts

The District did not have written procedures for creating, modifying or disabling user accounts. The Business Manager sends a form to the IT Department to request new user accounts. If any user accounts need to be disabled or modified, the Business Manager calls or e-mails the IT Department.

The Network Manager told us that he immediately disabled accounts for employees who left District employment, but did not periodically review the District's user account list. We reviewed all 109 enabled nonstudent network user

accounts, and all seven local user accounts on one server and six employee computers,[1] to determine whether the accounts were unneeded. We found that all seven of the local user accounts were needed.

However, we also found that nine nonstudent network user accounts (8 percent) were unneeded and should have been disabled. These accounts included five former employees' network accounts, one shared account and three generic accounts. The Network Manager told us he would deactivate these accounts.

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)[2] and compromise IT resources.

Why Should District Officials Develop a Written IT Contingency Plan?

An IT contingency plan typically includes an analysis of business processes and continuity needs, instructions, specific roles of key individuals and precautions needed to recover data and quickly resume operations in the event of an unplanned disruption.

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. These events can include power outages, software or hardware failures caused by a virus or other type of malicious software, human error, equipment destruction, or a natural disaster (e.g., flood, fire).

Testing and updating IT contingency plans is particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks. 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.

District Officials Did Not Develop a Written IT Contingency Plan

District officials did not develop a comprehensive written IT contingency plan to document and inform staff how they should respond to unplanned disruptions and disasters that affect the District's IT environment. 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.

1 Refer to Appendix B for further information on our sample selection.

2 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.

The District created full weekly backups of its IT system, which are stored off-site and off-network. However, these backups were not periodically tested to ensure that they will function as expected.

The Network Manager told us that SCRIC's system provided him with a daily summary of nightly backups performed by SCRIC. Therefore, he trusted that the District's backups were complete and usable. He also told us that, in the future, he could coordinate with the SCRIC to periodically test the backups.

In addition, the Network Manager provided us with the IT contingency plan that he started to develop in October 2021 – before our audit began – but it was not complete. The Network Manager told us that he did not know why the District did not have a plan in place before he became the Network Manager, but he understood the importance of having one.

Without a comprehensive written plan, the District has an increased risk that it could suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees, during a disruption or disaster.

However, these backups were not periodically tested to ensure that they will function as expected.

Why Should District Officials Compare Installed Software to a Software Inventory?

Software inventory management is essential for safeguarding school district assets and data, managing software updates and patches and complying with software licensing. Software inventory records should include software application descriptions, versions and serial numbers; descriptions and locations of computers on which the applications are installed; and pertinent licensing information for the applications. If school districts do not maintain a detailed, current software inventory list, then school district software and the data it contains can be exposed to an increased risk of misuse and/or loss.

Effective software management also includes periodically comparing installed software to an authorized software inventory list to ensure that only appropriate business software is installed. This helps reduce a school district's risk of experiencing unwanted consequences and paying unnecessary costs that could result from having unauthorized software, such as inadvertently violating copyright laws by having more software users than licenses for a particular application.

…[N]o one at the District periodically compared installed software to the inventory list.

District Officials Did Not Compare Installed Software to a Software Inventory

Although the Network Manager provided us with an authorized software inventory, no one at the District periodically compared installed software to the inventory list. We reviewed 72 of 425 software applications installed on six computers and two

servers[3] and found that only six of the software applications were on the software inventory. However, all 72 software applications were for appropriate District purposes. While the Network Manager did not find it necessary to compare installed software to the authorized software inventory list, without doing so, officials may not detect potential licensing violations and cannot ensure that only authorized software is installed.

As a result, the District has an increased risk that unauthorized software, including malicious software (malware), could be installed and remain undetected. Malware can gather sensitive information such as passwords without a computer user's knowledge, corrupt data or delete files, make devices inaccessible or inoperable, be expensive to fix and can cause significant losses in productivity until corrected.

What Do We Recommend?

The Board should:

1. Develop written procedures for granting, modifying and disabling user access to the network and computers and for periodically reviewing accounts to ensure they are needed.

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

District officials should ensure that the Network Manager:

3. Evaluates all existing network user accounts and disables any deemed unneeded.

4. Periodically tests data backups.

5. Confirms all installed software is authorized, ensures the authorized software inventory list is up to date and establishes procedures to periodically compare installed software to the authorized software inventory list.

3 See supra, note 1.

Appendix A: Response From District Officials

Unit Name: Franklin CSD
Audit Report Title: Information Technology
Audit Report Number: 2022M-19

Thank you for auditing the Franklin Central School District. Upon review of your findings, we would like to point out that the scope of the audit period coincides with the COVID-19 pandemic. During this time frame, our district information technology staff were supporting remote learning for students, staff, and parents for the first time in the district's history. This also included the rollout of 300 devices to students. The district is extremely proud of the IT department's efforts during these unprecedented times.

For each recommendation included in the audit report, the following is the corrective action(s) taken or proposed. For recommendations where corrective action has not been taken or proposed, we have included the following explanations.

Audit Recommendation:
Develop written procedures for granting, modifying and disabling user access to the network and computers and for periodically reviewing accounts to ensure they are needed.

Implementation Plan of Action:
Franklin CSD will work over the summer of 2022 to develop and implement a procedure that addresses these deficiencies.

Implementation Date:
Prior to the start of the 2022-23 school year.

Person Responsible for Implementation:
Network Manager

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

Implementation Plan of Action:
This plan creation is already in progress and was at the time of the audit. The IT department will work over the summer of 2022 to finalize this plan.

Implementation Date:
Prior to the start of the 2022-23 school year.

"Educating and empowering students to maximize their potential as learners and citizens"

Phone: 607-829-3551 Fax: 607-829-2101 P.O. Box 888 Franklin, NY 13775

Person Responsible for Implementation:
Network Manager

Audit Recommendation:
Evaluate all existing network user accounts and disable any deemed unneeded.

Implementation Plan of Action:
We have already begun this process and will review accounts quarterly.

Implementation Date:
Already implemented

Person Responsible for Implementation:
Network Manager

Audit Recommendation:
Periodically tests data backups.

Implementation Plan of Action:
The district will coordinate with SCRIC to test data backups annually.

Implementation Date:
Backup data restoration was successfully tested on 11 May 2022.

Person Responsible for Implementation:
Network Manager

Audit Recommendation:
Confirm all installed software is authorized, ensure the authorized software inventory list is up to date and establish procedures to periodically compare installed software to the authorized software inventory list.

Implementation Plan of Action:

The district believes current procedures are adequate. Users have no administrative rights and cannot install software. Additionally, the district has network policies and security software in place to prevent malicious software from running on individual devices.

Implementation Date:
N/A

Person Responsible for Implementation:

Network Manager

Signed:

5/12/22

Bonnie Johnson

Date

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

- We interviewed District officials and reviewed the District's IT policies to gain an understanding of IT operations, specifically those related to granting, modifying and disabling network and local user accounts and security settings and software, and to determine whether the District had an IT contingency plan.
- We ran specialized audit scripts on the District's domain controller,[4] on October 22, 2021, and analyzed the data produced to assess the necessity and appropriateness of network user accounts and security settings. We compared 109 nonstudent network user accounts to the active employee list to identify accounts of former employees and/or unneeded accounts. We followed up with the Network Manager to discuss potentially unneeded accounts.
- We used our professional judgment to review two of the District's seven servers, including the District's domain controller, and six computers with six nonstudent network user accounts. We chose to review these two servers and six computers based on the likelihood that they had access to PPSI. We ran specialized audit scripts on these servers and computers, on November 5, 2021, to examine the computers' local user accounts, security settings and software to determine whether they had any IT security weaknesses. We did not include the server that served as the District's domain controller in our review of local user accounts because it does not have any of these accounts. However, we included this server in our review of software applications to determine whether the applications installed on this device were for appropriate District purposes.

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.

4 The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain. It is responsible for allowing users to access Microsoft Windows domain resources.

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.

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

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