REPORT OF EXAMINATION | 2022M-151

Frankfort-Schuyler Central School District

Information Technology Assets and Network Access

DECEMBER 2022

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

Contents

Report Highlights

Frankfort-Schuyler Central School District

Audit Objective

Determine whether Frankfort-Schuyler Central School District (District) officials maintained appropriate information technology (IT) asset inventory records and established adequate controls over network user accounts.

Key Findings

District officials did not maintain appropriate IT asset inventory records or establish adequate IT controls over network user accounts. In addition to sensitive IT weaknesses communicated confidentially, District officials did not:

- Develop written procedures for tracking IT assets. Nine of 31 devices (laptops, desktops and tablets) we tested were not located.
- Adequately manage network user accounts. Sixty-five network user accounts were not needed.
- Enter into a service level agreement (SLA) with each of the District's IT service providers to clearly identify the IT services and providers' responsibilities. Over a half million dollars was paid to IT service providers.

In addition, because officials did not develop a written IT contingency plan there is an increased risk that the District could lose important data and suffer a serious interruption to operations, such as not being able to process paychecks, vendor payments, student grades or State aid claims.

Key Recommendations

- Establish adequate procedures, plans and agreements needed to protect the District's IT assets, network and data.

District officials generally agreed with our recommendations and initiated or indicated they planned to initiate corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

Background

The District serves the Towns of Frankfort and Schuyler in Herkimer County.

The District is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District's Assistant Superintendent of Business and Technology (Assistant Superintendent) and Superintendent are responsible for managing the District's IT operations, in conjunction with a Network Administrator and a computer technical assistant.

Quick Facts	
Active Nonstudent Devices	646
Enabled Nonstudent Network User Accounts	255
Cost of Third-Party IT Services for 2021-22	$526,000

Audit Period

July 1, 2020 – December 20, 2021

Information Technology Assets and Network Access

IT networks and systems are comprised of both physical IT assets and data which are valuable resources that support a school district's day-to-day operations such as maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI).[1] If a school district's IT network and systems are compromised or disrupted, the results could range from inconvenient to catastrophic and could require extensive efforts and resources to evaluate, repair and/or rebuild. While effective controls will not guarantee the safety of an IT network and systems, a lack of effective controls significantly increases the risk that physical IT assets such as hardware and software and the data accessed through the network may be lost or damaged by inappropriate access and use.

School district personnel should maintain detailed, up-to-date inventory records for IT assets.

The District contracts with the Mohawk Regional Information Center (MORIC) through the Madison-Oneida Board of Cooperative Educational Services, and Oneida-Herkimer-Madison Board of Cooperative Educational Services (OHM BOCES) for IT-related services. These services include: Internet access and filtering, firewall and intrusion detection, data support, financial and student information system support, network administration and security awareness training. As part of these IT related services, MORIC provides the District with a Network Administrator and OHM BOCES provides a computer technical assistant, who both work three days a week at the District.

How Should a School District Maintain IT Asset Inventory Records?

School boards should adopt written inventory policies and school district officials should implement controls to ensure IT assets are accounted for, properly safeguarded and disposed of appropriately when applicable. School district personnel should maintain detailed, up-to-date inventory records for IT assets. These records should identify and track an IT asset through its life cycle, including acquisition, use and disposal.

At a minimum, the inventory records should include a description of each item, including make, model and serial number; the name of the person to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase information including acquisition date and original cost. Each item also should be immediately affixed with an identification tag and entered into the inventory records upon receipt by the school district. Inventory records should be updated when assets are moved or reassigned to another person to help ensure the records are accurate and the assets can be located.

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 individual or entities.

In addition, school district officials should conduct periodic physical inventories of IT assets. The results should be compared to detailed inventory records and any resulting discrepancies should be investigated. The disposal of IT assets or donation to other school districts should be authorized by the school board and documented prior to the actual disposition of the items and their removal from the inventory records. Because these assets could contain sensitive information or provide access to the school district's network, the assets should be stored in secure areas with limited access when not in use or awaiting disposal.

The District Did Not Maintain Adequate IT Asset Inventory Records

The District's inventory policy (not specific to IT assets) states that all District personal property having a unit resale of $250 or more shall be inventoried once annually. The policy further states that procedures will be established to ensure that any equipment received by the District is logged, its physical location identified and it is properly labeled with an inventory tag.

However, the Superintendent and Assistant Superintendent have not developed any supplemental written procedures to address the maintenance of detailed, up-to-date inventory records for IT assets, including the type of information that should be included in the records, comparisons of the inventory records to physical inventory counts and the required approvals and safeguards for asset disposals.

The Network Administrator and computer technical assistant were responsible for tagging District IT assets when they were received and maintaining and updating the District's inventory records for IT assets. The Network Administrator provided us with an IT inventory report that included 646 active devices (laptops, desktops and tablets) that were not assigned to students. The report did not always clearly identify to whom the device was assigned, the device's location (building, floor or room) and did not include the purchase price for any of the devices.

We selected a sample of 31 IT devices from the inventory report and, with the assistance of the Network Administrator, attempted to trace them to their physical locations at the District. The Network Administrator was unable to locate nine devices (29 percent). While we found the remaining 22 devices, five of them were found in a different location than was listed in the IT inventory report.

These discrepancies were not detected because officials and IT staff did not perform annual physical inventories of IT assets to help ensure the inventory records were accurate and the assets were on hand. In addition, the inventory records did not always provide a clear location for the assets and the records were not always updated when the assets were moved to different locations or reassigned. Without complete and accurate inventory records and periodic physical inventories, the District's IT assets are at an increased risk of loss, theft

or misuse. Additionally, in the event of a disaster, the District would be unable to provide its insurance company with an accurate list of assets to replace including the equipment's cost.

Furthermore, the Assistant Superintendent and Network Administrator did not have adequate procedures to collect and secure old IT devices when they were replaced and to obtain Board authorization for the disposal of IT assets. After we inquired about the District's process for disposing of IT assets, the Network Administrator retrieved 22 laptops from throughout District buildings and moved them to the technology office for storage while they await recycling. The Network Administrator told us these laptops were replaced during the summer of 2020 when teachers were off, so he left them in the classrooms to allow teachers to remove any files they needed. He told us he collected some old laptops as he came across them, but he did not begin to actively retrieve and secure these laptops until our audit. Because of the lax procedures for collecting the older laptops when they were replaced, there was an increased risk the assets could be stolen or that PPSI could be compromised if an unauthorized user was able to gain access to a laptop and its related data.

According to the IT inventory report, 99 IT devices were disposed of from July 1, 2020 through October 31, 2021. The records indicate 12 of these devices were computers that were donated to another public school district where the Network Administrator also works. The Network Administrator told us he obtained the Assistant Superintendent's verbal approval to donate the computers because the District was going to recycle them and the other school district could use them. We confirmed with the Assistant Superintendent that she approved this donation.

However, there was no indication that the Board approved the disposal or donation of the 99 devices. According to Board meeting minutes, the last time the Board approved the disposal of IT assets was in December 2019 (prior to our audit period). The Assistant Superintendent and Network Administrator did not provide an explanation for why they did not request Board approval to dispose of and donate these devices. Prior Board approval for asset disposal is important because it helps ensure that disposal of equipment only occurs when the equipment is unneeded, unusable or obsolete.

District officials acknowledged that although they have a process to keep track of IT assets, the process was not formalized in written procedures, and they did not always comply with the process. They indicated that they will formalize their process and improve the way they maintain physical IT assets and the related inventory records.

How Should School District Officials Manage Network User Accounts and Access?

Network user accounts enable networks, connected computers and certain applications to recognize specific users and processes and provide user accountability by affiliating network user accounts with specific users and processes. Network user accounts are potential entry points for attackers because, if compromised, they could be used to access and then view, modify and/or delete data on the network.

School district officials are responsible for restricting network user account access to only those network resources and data needed by the user to complete job duties and responsibilities. Restricting network user access helps ensure data and IT assets are safeguarded and protected from unauthorized use and/or modification. Officials should develop and implement written procedures for granting, changing and revoking user access to the network. These procedures should establish who has the authority to grant or change access (e.g., department manager approval) and allow users to access only what is necessary to complete their job duties and responsibilities.

To minimize the risk of unauthorized access, officials should actively manage network user accounts including their creation, use and dormancy. When employees leave school district employment, or when user accounts are otherwise no longer needed, officials should ensure that these accounts are disabled in a timely manner. Officials should also regularly monitor network user accounts to ensure they are appropriate and authorized.

Officials should limit the use of service and shared user accounts and routinely evaluate the need for the accounts and disable those that are not related to a current school district or system need. Service and shared network user accounts are not linked to one individual and therefore may have reduced accountability. Service user accounts are accounts created for the sole purpose of running a particular network or system service or application. For example, service accounts may be created and used for automated backup or testing processes, or generic email accounts such as a service help desk account. Shared user accounts are accounts with a username and password that are shared among two or more users and are often used to, for example, provide access to guests and other temporary or intermittent users.

District Officials Did Not Adequately Manage Network User Accounts and Access

The District's policy on responsible use of digital information systems states that the Superintendent is authorized to develop and adopt procedures for assigning, reviewing and removing user access rights. According to the policy, these

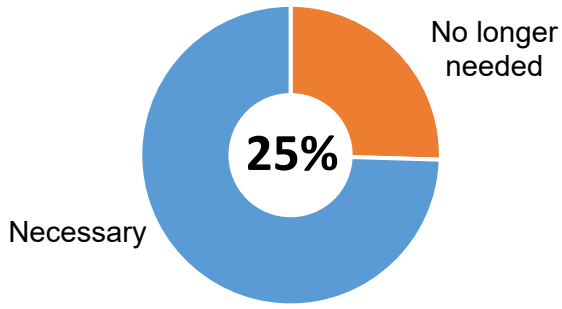
procedures should establish who has the authority to grant or change access and they should include protocols for removing users from the system when an individual is no longer affiliated with the District.

The Superintendent has not developed written procedures for granting, changing and revoking user access to the network. The Assistant Superintendent usually emails the Network Administrator or computer technical assistant when a user's access rights need to be added, modified or removed. However, based on our audit testing, this process was not effective in ensuring network user accounts were disabled timely when they were no longer needed. In addition, the Assistant Superintendent and Network Administrator did not regularly review the enabled network user accounts to identify user accounts that were not needed and disable them.

We reviewed all 255 enabled nonstudent network user accounts for necessity and appropriateness. With the assistance of the Network Administrator and Assistant Superintendent, we determined 65 of the 255 network user accounts (25 percent) were unneeded (Figure 1).

FIGURE 1

Nonstudent Accounts



Twenty-four of the 65 unneeded user accounts belonged to former employees or third-party consultants who no longer worked for or provided services to the District. The remaining 41 unneeded accounts were service accounts or shared by two or more users.

Of the 65 unneeded accounts, eight had never been used to log in to the network. An additional 46 accounts had not been used in the last six months, including 18 accounts that last accessed the network prior to January 2019.

These unneeded network accounts were not identified sooner because the District's IT Department did not have effective procedures in place to promptly

disable user accounts when they were no longer needed and regularly review the accounts to determine their necessity.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could be used to inappropriately access and then view, modify and/or delete PPSI and compromise IT resources. Additionally, when a school district has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access.

Why Should a School District Have an SLA With Its Service Provider?

To help protect a school district's IT assets and network and avoid potential misunderstandings, school district officials should have a written SLA with the school district's IT service provider that clearly identifies the school district's needs and service expectations and includes provisions relating to confidentiality and protection of PPSI. An SLA establishes comprehensive, measurable performance targets and remedies for not meeting those requirements so that there is a mutual understanding of the nature and required level of services to be provided.

It provides detailed explanations of the services to be performed by identifying: the parties to the agreement and defining terminology; duration of the agreement, scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment. There should be no uncertainty about what the IT service provider will deliver, when it will be delivered or how much it is going to cost. A vague agreement can lead to additional or increasing costs that were not expected.

The SLA should be reviewed by a school district's legal counsel and IT staff, as appropriate. It should be periodically reviewed, especially if the IT environment or needs change significantly. Developing a good SLA takes some effort but can help avoid potentially costly misunderstandings and establish an efficient and secure environment for IT assets and network access.

District Officials Did Not Have Adequate SLAs

District officials did not establish comprehensive SLAs with MORIC and OHM BOCES to identify the responsibilities and specific services to be provided because the Superintendent and the Assistant Superintendent were not aware of the benefits of having such agreements.

We asked the Assistant Superintendent to provide us with detailed documentation and cooperative service agreements with descriptions of IT services provided by MORIC and OHM BOCES. The Assistant Superintendent provided us

There should be no uncertainty about what the IT service provider will deliver, when it will be delivered or how much it is going to cost.

with a “Service Request Form and Contract” for MORIC and a “Final Service Commitment Form” for OHM BOCES. The documents do not:

- Provide detailed information for services to be provided to the District,
- Explain the District’s, MORIC’s and OHM BOCES’ responsibilities, or
- Include comprehensive, measurable performance targets.

As a result, the documents were not as detailed as SLAs could be. For the 2021-22 fiscal year, the District paid approximately $526,000 to MORIC and OHM BOCES, $471,000 and $55,000, respectively, for IT products and services.

Without adequately written SLAs, the District and MORIC and OHM BOCES did not have stated responsibilities for key IT controls such as software and user account management, or user account monitoring are not clearly defined. This can contribute to confusion over who has responsibility for the various aspects of the District’s IT environment, which could put the District’s IT assets and network, including PPSI at greater risk for unauthorized access, misuse or loss.

How Does an IT Contingency Plan Help Protect and Secure IT Assets and Network Access?

A well designed, adopted and tested IT contingency plan helps officials recover a school district’s IT systems and operations from an unplanned disruption. The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of a school district’s computerized operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident.

The critical components of a comprehensive written IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Written policies and procedures for computer backups are also critical components and help ensure that information is routinely backed up and available in the event of a disruption.

The IT contingency plan can also include, among other items deemed necessary by school district officials, the following:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel’s responsibilities,
- Communication protocols with outside parties,
- Prioritized mission critical processes,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,

- Backup methods and storage policies, and
- Details concerning how the plan will be periodically tested and updated.

The District Did Not Have an IT Contingency Plan

The Board and District officials did not develop and adopt a comprehensive written IT contingency plan. The Assistant Superintendent stated that she thought that that MORIC's IT contingency plan was sufficient to address the District's needs. However, District officials did not review MORIC's IT contingency plan to determine if the District's needs would be met and did not have a copy of this plan. As a result, District officials and employees have insufficient written guidance to follow to restore, resume and/or rebuild essential operations in a timely manner or to help minimize damage and recovery costs after an unexpected IT disruption.

An unexpected IT disruption could include a power outage, software failure caused by a virus or other type of malicious software, a ransomware attack, equipment destruction, inadvertent employee action or a natural disaster, such as a flood or fire. Without a comprehensive written IT contingency plan, there is an increased risk that the District could lose important data and suffer a serious interruption to operations, such as not being able to process paychecks, vendor payments, student grades or State aid claims.

The Board may adopt a plan that incorporates elements of MORIC's plan as appropriate; however, the Board and District officials must evaluate the District's critical business processes and services and develop a plan that addresses its own unique IT operations. For example, the plan should address how employees will communicate, where they will go and how they will continue to do their jobs during a disruption. Personnel expected to execute the plan must understand the plan and their responsibilities if a disruption occurs.

What Do We Recommend?

The Board and District officials should:

1. Develop detailed SLAs with the District's IT service providers to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties. Ensure that the agreements include measurable performance targets, remedies if those targets are not met and the related costs.

2. Develop and adopt a comprehensive written IT contingency plan that provides adequate guidance on how the District plans to recover its critical IT operations in the event of an unexpected incident. Distribute the plan to all responsible parties and ensure that it is periodically tested and updated as needed.

The Superintendent and Assistant Superintendent should:

3. Develop written procedures for tracking and inventorying IT assets. The procedures should address maintaining detailed inventory records (including the specific information that should be recorded), tagging of items when received, updating the inventory records for changes in locations or assignments, the requirements for asset disposals and performing annual physical inventories.

4. Ensure the District's IT asset inventory records include the detail necessary to adequately track and locate IT assets, including cost, acquisition date, building and room number and, if applicable, the name of the person to whom the equipment is assigned.

5. Ensure an annual physical inventory of IT assets is performed and the results are compared to the inventory records. Take appropriate action to follow up on any discrepancies.

6. Ensure that proper authorization is obtained from the Board prior to the disposal or donation of IT assets and removal from the inventory records.

7. Develop and adhere to written procedures for granting, changing and disabling network user account access. The procedures should specifically address how the District will identify network user accounts that are no longer needed so they can be disabled in a timely manner.

The Network Administrator should:

8. Perform a physical inventory of IT equipment, attempt to locate any missing equipment and update inventory records accordingly.

9. Promptly recover and secure IT assets that have been replaced and are awaiting disposal.

10. Evaluate all enabled network accounts, disable any deemed unneeded and periodically review all network user accounts for necessity.

Appendix A: Response From District Officials

Frankfort-Schuyler Central School District
605 Palmer Street Frankfort, NY 13340 | 315-894-5083 Superintendent |315-895-7781 Business Office |

December 12, 2022

Board of Education
Frankfort-Schuyler CSD

RE: Draft IT Audit Response

Members of the Board of Education,

Below is the district response to the draft report issued by the State Comptroller's Office, their recommendation is noted as well as the districts response.

Comptroller Recommendation #1- Develop detailed SLA's with the district's IT service providers to address the District's specific needs and expectations for IT services and the roles and responsibilities of all parties. Ensure that the agreements include measurable performance targets, remedies if those targets are not met and the related costs.
District Response #1- The district has requested such documents from the BOCES and RIC providers. These documents do not exist. The district is being told that it is a work in progress at the RIC and BOCES. When the district contracts with the RIC and BOCES, an initial service request, per COSER, is completed. This request lists the COSER, Service Title and cost. In addition a catalog with a brief description of the service is available, however, not a SLA as recommended by NYS Office of the State Comptroller.
Implementation Date: Unknown
Person Responsible for Implementation: MORIC, BOCES

Comptroller Recommendation #2- Develop and adopt a comprehensive written IT contingency plan that provides adequate guidance on how the district plans to recover its critical IT operations in the event of an unexpected incident. Distribute the plan to all responsible parties and ensure that it is periodically tested and updated as needed.
District Response #2- While the district did have a plan for disaster recovery as they work directly with the RIC as part of the services they provided, it was not officially documented. As of the date of the Comptrollers Exit Conference on December 12, 2022, the district in collaboration with the MORIC has developed a DRAFT written disaster recovery plan as well as a Cybersecurity Incident Response Plan. These plans are in their second read at this time, with full adoption by the Board of Education expected by June 2023.
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians, MORIC

Middle-Senior High School
605 Palmer Street
315-895-7461 Principal
315-895-4032 Fax
315-895-7733 Special Education

FRANKFORT-SCHUYLER Pride

Frankfort-Schuyler Elementary School
610 Reese Road
315-895-7491 Principal
315-895-4102 Fax
www.frankfort-schuyler.org

Comptroller Recommendation #3- Develop written procedures for tracking and inventorying IT assets. The procedures should address maintaining detailed inventory records (including specific information that should be recorded), tagging of items when received, updating the inventory records for changes in locations or assignments, the requirements for asset disposals and performing annual physical inventories.

See Note 1 Page 15

District Response #3 While the district does perform an annual physical inventory in house annually during the summer months, as well as a full physical inventory with an outside agency approximately every five years, this procedure was not officially documented. As of the date of the Comptrollers Exit Conference on December 12, 2022, the district in collaboration with the MORIC has developed a written Physical Device Procedure.
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians. MORIC

Comptroller Recommendation #4- Ensure the district's IT asset inventory records include the detail necessary to adequately track and locate IT assets, including costs, acquisition date, building and room number and, if applicable, the name of the person to whom the equipment is assigned.
District Response #4 While the district does perform an annual physical inventory in house annually during the summer months, as well as a full physical inventory with an outside agency approximately every five years, this procedure was not officially documented. All assets are tracked currently in [redacted], albeit absent the cost. As of the date of the Comptrollers Exit Conference on December 12, 2022, the district in collaboration with the MORIC has developed a written Physical Device Procedure. This procedure notes the name, category, serial number, tag number, assigned location and cost will now be added to all assets. All tracked in a tracking software (currently [redacted]).
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians, MORIC

Comptroller Recommendation #5- Ensure an annual physical inventory of IT assets is performed and the results are compared to the inventory records. Take appropriate action to follow up on any discrepancies.
District Response #5 While the district does perform an annual physical inventory in house annually during the summer months, as well as a full physical inventory with an outside agency approximately every five years, this procedure was not officially documented. All assets are tracked currently in [redacted], albeit absent the cost. As of the date of the Comptrollers Exit Conference on December 12, 2022, the district in collaboration with the MORIC has developed a written Physical Device Procedure. This procedure notes the name, category, serial number, tag number, assigned location and cost will now be added to all assets. All tracked in a tracking software (currently [redacted]).
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians, BOCES, MORIC

Comptroller Recommendation #6- Ensure that proper authorization is obtained from the board prior to the disposal of donation of IT assets and removal from the inventory records.
District Response #6 It is currently the districts practice to approve all disposals through the Board of Education, however, there were instances where this was missed. The district has reiterated and will continue to reiterate with it's IT staff that all disposals are to be Board Approved prior to the disposal of the items.
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians

Comptroller Recommendation #7- Develop and adhere to written procedures for granting, changing and disabling network user accou access. The procedure should specifically address how the district will identify network user accounts that are no longer needed so they can be disabled in a timely manner.
District Response #7- As of the date of the Comptrollers Exit Conference on December 12, 2022, the district has implemented a new h onboarding and off boarding official form to be used for all users on the system.
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians, MORIC

Comptroller Recommendation #8- Perform a physical inventory of IT equipment, attempt to locate any missing equipment and update inventory records accordingly.
District Response #8- While the district does perform an annual physical inventory in house annually during the summer months, as w as a full physical inventory with an outside agency approximately every five years, this procedure was not officially documented. All asse are tracked currently in [redacted], albeit absent the cost. As of the date of the Comptrollers Exit Conference on December 12, 2022, the district in collaboration with the MORIC has developed a written Physical Device Procedure. This procedure notes the name, category, serial number, tag number, assigned location and cost will now be added to all assets. All tracked in a tracking software (currently [redacted]).
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians, BOCES, MORIC

Comptroller Recommendation #9- Promptly recover and secure IT assets that have been replaced and are awaiting disposal.
District Response #9- The district does its best to find secure locked locations to store these assets while awaiting disposal. Sometime storage space is limited, but items should always be behind locked doors.
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians

Comptroller Recommendation #10- Evaluate all enabled network accounts, disable any deemed unneeded and periodically review all network user account for necessity.
District Response #9- As of the date of the Comptrollers Exit Conference on December 12, 2022, the district in collaboration with the MORIC has reviewed all user accounts on the network and [redacted] for older users, both students and staff. All older users have be made inactive. This "audit" will take place at the school level on an annual basis going forward.
Implementation Date: Fiscal Year 2022-2023
Person Responsible for Implementation: Assistant Superintendent of Business & Technology, IT Technicians. MORIC

Frankfort-Schuyler Central School District
605 Palmer Street Frankfort, NY 13340 | 315-894-5083 Superintendent |315-895-7781 Business Office |

Additional District Response: During the 2022-2023 fiscal year, the district has contracted with the MORIC Data Privacy and Security Team to provide an additional level of auditing on all IT systems to ensure the district is implementing the most up to date standards and review processes. This service not only assists with user audits, but also the following:

- Improve Compliancy with State and Federal Laws and Regulations
- Begin the NSIT Cybersecurity Framework Implementation
- Develop and Maintain comprehensive Data Privacy and Security Plans
- Review User Access and Permissions for all Administrative Systems
- Create Trainings Campaigns for Staff Focused around Data Privacy & Security
- Schedule and evaluate vulnerability scans of the districts network
- Monitor and Refine hardware and software inventory procedures
- Analyze scanning data to mitigate potential threats to create a vulnerability management program

The district would like to thank the comptroller's office for their time and effort to review the districts IT processes and look forward to the implementation of the corrective action plan.

Should you have any further questions, please feel free to contact me.

Best,

Kacey Sheppard, CFE, SDBL, SDL
Assistant Superintendent of Business & Technology
315-895-7781
ksheppard@frankfort-schuyler.org

Appendix B: OSC Comment on the District's Response

Note 1

District officials were unable to provide appropriate evidence that they performed a physical inventory of IT assets.

Appendix C: 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 IT staff, and reviewed the District's IT policies and procedures to gain an understanding of the IT environment, inventory records maintained for IT assets, the management of network user accounts and permissions and to determine whether the District had an IT contingency plan.
- We requested a fixed asset inventory report, which we received on November 12, 2021. Using our professional judgment, we selected 31 devices (laptops, desktops and tablets) that were not assigned to students. Our sample included devices with various purchase dates that showed locations in different buildings as well as some that had no location listed. With the assistance of IT Department staff, we attempted to physically locate the IT devices in District buildings.
- We ran a computerized audit script on the District's domain controller, on September 29, 2021, to gather network user account information. We then analyzed the results generated from the script to obtain information about the District's 255 enabled nonstudent network user accounts, including their permissions, to determine whether they were necessary and appropriate. We compared the 255 nonstudent network user accounts to the active employee list to identify whether there were enabled accounts related to former employees and other accounts that may be unneeded. We followed up with the Network Administrator and the Assistant Superintendent to assess whether the accounts were needed.
- We requested copies of any SLAs that the District had with MORIC and OHM BOCES and reviewed the documents provided.

Our audit also examined the adequacy of certain other 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.

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 D: 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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief of Municipal Audits

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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