

# Waterville Central School District

## Network User Accounts and Information Technology Contingency Planning

---

NOVEMBER 2022

---



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

# Contents

---

- Report Highlights . . . . . 1**
  
- Network User Accounts and Information Technology  
Contingency Planning . . . . . 2**
  - How Should District Officials Manage Network User Accounts  
and Permissions? . . . . . 2
  
  - Officials Did Not Adequately Manage Network User Accounts  
and Permissions . . . . . 3
  
  - Why Should a District Adopt a Written IT Contingency Plan? . . . . . 7
  
  - The District Did Not Have a Written IT Contingency Plan . . . . . 8
  
  - What Do We Recommend? . . . . . 8
  
- Appendix A – Response From District Officials . . . . . 10**
  
- Appendix B – Audit Methodology and Standards . . . . . 14**
  
- Appendix C – Resources and Services . . . . . 16**

# Report Highlights

## Waterville Central School District

### Audit Objective

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

### Key Findings

District officials did not adequately manage network user accounts or develop a written IT contingency plan that details how District officials would respond to IT disruptions. As a result, officials had active but unneeded network user accounts that could be used as entry points for individuals to gain unauthorized access to the District's IT systems, and the lack of a comprehensive written IT contingency plan impairs the District's ability to recover from an unexpected IT disruption.

In addition to finding sensitive IT control weaknesses that were confidentially communicated to officials, we found that officials did not:

- Develop written procedures for granting, changing and disabling user access rights to the network.
- Perform periodic reviews of all network user accounts to determine whether they were appropriate or needed. As a result, 11 percent of the District's non-student user accounts were unneeded and should have been disabled.

### Key Recommendations

- Develop written network user account access procedures and periodically review and evaluate all network user accounts.
- Develop and adopt a comprehensive written IT contingency plan.

District officials generally agreed with our recommendations and indicated they have taken or plan to take corrective action.

### Background

The District serves the Towns of Brookfield and Madison in Madison County and the Towns of Augusta, Kirkland, Marshall, Paris, Sangerfield and Vernon in Oneida County.

An elected seven-member Board of Education (Board) is responsible for the general management and control of financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and, along with other administrative staff, is responsible for day-to-day management under the Board's direction.

The District's Business Official serves as the IT Director (Director). The District contracts with the Mohawk Regional Information Center (MORIC) through the Oneida-Herkimer-Madison Board of Cooperative Educational Services (BOCES) to provide various IT services, including network configuration support. BOCES provides the District with a network administrator (Administrator) who is responsible for managing the District's network and user accounts.

#### Quick Facts

Network User Accounts	
Employees	201
<b>Non-Students:</b>	
Needed	<b>300</b>
Unneeded	<b>38</b>
<b>Total</b>	<b>338</b>
<b>2021-22 Fiscal Year</b>	
BOCES IT Service Contract	\$415,000
Budgeted Appropriations	\$19 million

### Audit Period

July 1, 2020 – April 4, 2022

# Network User Accounts and Information Technology Contingency Planning

---

## How Should District Officials Manage Network User Accounts and Permissions?

School district officials are responsible for restricting network user account access to only those network resources and data needed by the user for learning and to complete their job duties and responsibilities. A school district should have written procedures for granting, changing and disabling user access and permissions to the network. This helps ensure data is safeguarded and protected from unauthorized use and/or modification.

Officials should disable unnecessary accounts when there is no longer a need for them because when unneeded network user accounts exist, the school district has an increased risk that personal, private and sensitive information could be intentionally or unintentionally changed and/or compromised by unauthorized individuals. Officials should also regularly review enabled network user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are still needed. Furthermore, when user accounts are provided for temporary work or guests, the accounts should have an expiration date to automatically terminate access after a designated and authorized period of time.

Service accounts are created for the sole purpose of running a particular network, system service or application and should be limited in use, as they are not linked to individual users and may have reduced accountability. For example, service accounts may be created and used for automated backup, testing processes or generic email accounts, such as a service help desk account. In addition to limiting the use of service accounts, officials should routinely evaluate the need for the accounts and disable those not related to a current district or system need.

Officials should have procedures to monitor who uses shared accounts and when and how they are used. Shared user accounts are accounts with usernames and passwords that are shared among two or more users and can be used to provide access to guests and other temporary or intermittent users (e.g., substitute teachers and contracted vendors). Since shared accounts are not assigned to an individual user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. If shared accounts are needed, each user should have and use their own network user account, this helps ease management and ensure accountability over work performed and data changed or deleted.

Officials must regularly review administrative accounts and promptly disable them when they are no longer needed. Generally, a network administrative account has permissions to monitor and control a network, connected computers and certain applications with the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide

---

changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, any program that a user with administrative permissions runs could inherently run with the same permissions. For example, if malicious software (malware) infected a computer, it may run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of network or computer compromise and/or data loss.

School district officials and IT staff should collectively have sufficient experience with the IT environment and have knowledge of the cybersecurity risks and threats which should be treated like any other hazard a school district may encounter along the way. This is particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks currently facing school districts. School district officials should identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the board, the superintendent and the IT department.

### **Officials Did Not Adequately Manage Network User Accounts and Permissions**

The District relies on its IT network and systems to support its day-to-day operations such as maintaining financial, personnel and student records, much of which contain personal, private and sensitive information (PPSI).<sup>1</sup> District network user accounts provide access to the networks, connected computers and certain applications. Network user accounts are potential entry points for attackers because they could be used to access and view, modify and/or delete data on the network.

Users of the District's network and associated systems include employees (staff and substitutes), students, and contractors (i.e., BOCES, MORIC, capital project vendor). The Administrator is responsible for granting, modifying and disabling user access to the network.

We reviewed all 338 enabled non-student network user accounts, including 159 assigned to District employees, 104 assigned to contractors, 68 service accounts and seven shared accounts. District officials did not adequately manage network

---

Cybersecurity risks... should be treated like any other hazard a school district may encounter along the way.

---

---

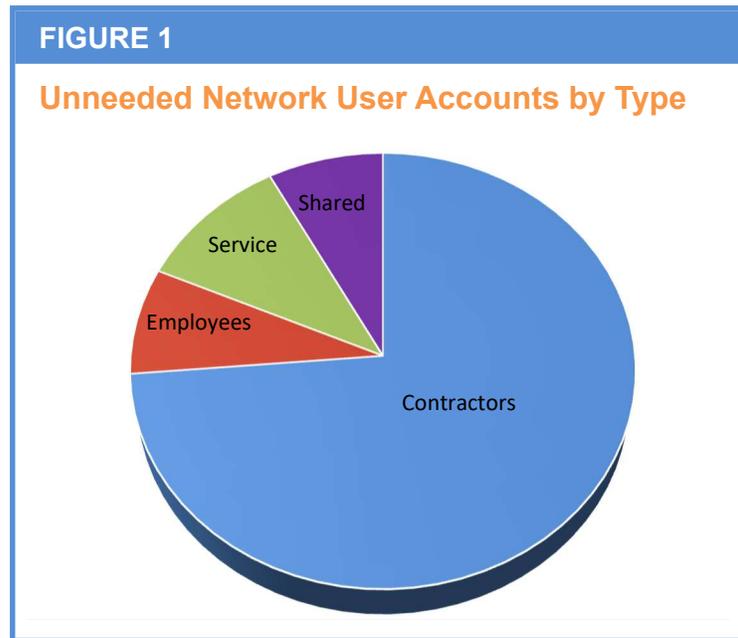
<sup>1</sup> PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, students, third parties or other individuals or entities.

user accounts. While the District had an employee event form that was used to notify the Administrator of staff changes,<sup>2</sup> it did not have written procedures for creating, modifying or disabling user accounts for all network user account types. As a result, we found that the District had unneeded contractor, employee, shared and service accounts that had not been disabled and/or monitored, and some contractor user accounts that had unnecessary administrative permissions to the network. In total, we identified 38 unnecessary network user accounts, as indicated in Figure 1.

Unneeded Contractor Accounts – The District does not have written procedures for adding or disabling network user accounts assigned to BOCES and MORIC staff or other contractors. Generally, when other contractors need network access, the Director emails the Administrator to create a network user account. When contractors no longer need network access, the Director told us that she is supposed to notify the Administrator to disable the contractor’s account. However, the Director did not always provide this notification.

For BOCES staff whose network accounts need to be enabled or disabled, the Administrator receives an email from the staff’s respective BOCES supervisor informing the

Administrator of the staff changes. The Administrator then updates the network user accounts based on these emails. In addition, the Administrator told us that they annually review BOCES network user accounts by comparing a BOCES employee list to the District’s enabled network user accounts, and the Administrator contacts the BOCES staff supervisors to determine who still needs access to the District’s network.



<sup>2</sup> The form lists the employee’s name, title, status (appointed, resigned, retired, terminated) and effective date. Based on the employee’s title, the Administrator assigns the employee access rights to various folders and email.

---

During our review of the 104 enabled network user accounts assigned to contractors, we found 28 network user accounts (27 percent) that should have been disabled. Nine of these unneeded network user accounts also had administrative permissions because MORIC and BOCES staff had previously used these accounts to provide IT support services to the District.

- Of the 20 BOCES unneeded network user accounts, four of these accounts had administrative permissions to the District's network. The Administrator told us that the BOCES supervisor did not notify them of the BOCES staff who no longer provided IT support or worked directly with the District's students.
- Of the seven MORIC unneeded network user accounts, five of these accounts had administrative permissions to the District's network. According to the Administrator, MORIC manages the network user accounts assigned to its staff. However, the Director and the Administrator did not ensure that unneeded MORIC staff accounts were disabled timely.
- For the one capital project vendor unneeded network user account, the Director did not notify the Administrator of the vendor's departure in July 2020.

Because the Director and the Administrator did not adequately monitor contractor network user accounts, there were unneeded network accounts that, in some cases, had administrative permissions which put the District at greater risk of those network accounts being compromised. For those network user accounts with administrative permissions, which allow a higher level of access, if they are compromised by a malicious individual, that person would have those same elevated permissions and could potentially cause more damage. Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could disrupt network communications that are critical to normal school district functions, especially given the ongoing and increasingly sophisticated threat of ransomware attacks.

Unneeded Employee Accounts – When a new employee is hired, the District Clerk provides the Administrator with a completed employee event form requesting that the employee be given a network user account and access rights to various network folders and email. Similarly, as soon as an employee leaves the District, the District Clerk should provide the event form to the Administrator, who should disable the employee's network user account.

For substitute employees, there are no written procedures for adding or disabling network user accounts. However, the Administrator reviews the Board's annual re-organizational meeting minutes to determine whether a substitute employee network user account needs to be added to or disabled from the network. In addition, the Administrator entered user account expiration dates for long-term

---

substitutes if an end date is indicated. When these dates are entered, the system automatically disables the user account's access rights as of the specified expiration date.

Our review of 159 enabled network user accounts assigned to employees disclosed that, generally, these users were District employees. However, we found three accounts assigned to former employees – a webmaster, bus driver and long-term substitute teacher. We discussed these three user accounts with the Administrator, who subsequently disabled them.

The webmaster's user account was created in 2017 for email only and we did not find any evidence that he used the account to access network resources using a District computer. The webmaster's role was reassigned in the fall of 2021, so the user account was no longer needed. The bus driver left District employment in March 2019. The District Clerk told us the bus driver left employment before the District began using the event form and the Administrator was not notified of the departure. The substitute was appointed in the 2020-21 school year as a teacher for the District's summer enrichment program through July 30, 2021. The Administrator did not include an expiration date in the system and did not realize the substitute teacher was not reappointed at the July 2021 annual re-organizational meeting, so the user account was not disabled.

User accounts of former employees that have not been disabled timely could potentially be used by those individuals or others for malicious purposes.

Unneeded Shared Accounts – The District had seven enabled shared network user accounts and, although four of the accounts were needed, the Administrator did not have procedures in place to monitor who used any of these accounts. The remaining three shared accounts were not necessary – one account was used for coaches to report scores, another was used for elementary news reporting and the third was used by the outdoors club for fundraising. These accounts have not been used since February 2018 as the District now uses other methods to communicate and share this information.

Shared network user accounts that are not disabled when they are no longer needed are another avenue for malicious individuals to attempt to use to disrupt the network.

Unneeded Service Accounts – Of the 68 network service accounts reviewed, four service accounts were for services that were no longer needed or used on the District's network. One account had been used to test student network accounts, another had been used for copier configuration and two accounts were used to re-route and migrate email service for an individual and the District, respectively.

---

According to the Administrator, no one routinely reviewed shared and service accounts. Neither the Director nor Administrator were aware these accounts were no longer needed to serve a business purpose for the District. If procedures were in place, they may have addressed who was responsible for periodically reviewing these accounts.

As a result of our audit, the Administrator disabled all 38 unneeded contractor, employee, shared and service accounts. Because the District's network had unneeded but still enabled network user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to potentially access data and compromise IT resources. In addition, compromising a network user account with administrative permissions could cause greater damage than compromising a lesser-privileged account because administrative accounts have full control over the network.

### **Why Should a District Adopt a Written IT Contingency Plan?**

An IT contingency plan is a school district's recovery strategy, composed of the procedures and technical measures that help enable the recovery of operations and data after an unexpected IT disruption. An unexpected IT disruption could include inadvertent employee action, a power outage, software failure caused by a virus or other type of malicious software, equipment destruction or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such an event. The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the school district's operations. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident and could significantly reduce the resulting impact.

The goal of an IT contingency plan is to enable the recovery of an IT system and/or electronic data as quickly and effectively as possible following an unplanned disruption. A comprehensive written IT contingency plan should focus on strategies for sustaining a school district's critical business processes in the event of a disruption. The critical components of a comprehensive IT contingency plan establish technology recovery strategies and should consider the possible restoration of hardware, applications, data and connectivity. Written policies and procedures are also critical components and help ensure that information is routinely backed up and available in the event of a disruption.

---

Neither the Director nor Administrator were aware these accounts were no longer needed to serve a business purpose for the District.

---

---

Typically, an IT contingency plan should address the following key components:

- Roles and responsibilities of key personnel,
- Periodic training regarding the key personnel's responsibilities,
- Identifying and prioritizing critical business processes and services,
- Communication protocols with outside parties,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,
- Detailed backup procedures, and
- Details concerning how the plan will be periodically tested and updated.

### **The District Did Not Have a Written IT Contingency Plan**

District officials did not develop a written IT contingency plan to describe the procedures and technical measures officials would take to respond to potential disruptions and disasters affecting the District's IT environment. While MORIC has a written disaster recovery plan that includes disaster recovery procedures for the District's applications and the domain controller, the Board did not adopt its own IT contingency plan that addresses technical needs and situations unique to the District.

The Director told us officials were unaware they needed to develop their own IT contingency plan because BOCES manages the District's network. While the Board may adopt a plan that incorporates the MORIC disaster recovery plan, the Board should adopt its own IT contingency plan that addresses the District's own unique IT operations and test the plan to help ensure services can continue in the event of a disruption or disaster. Without a comprehensive 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.

### **What Do We Recommend?**

The Board and District officials should:

1. Develop written procedures for granting, changing and disabling user access to the network, including procedures to disable any unneeded accounts when they are no longer needed and to periodically review and monitor all network user accounts for necessity.

---

The Director told us officials were unaware they needed to develop their own IT contingency plan because BOCES manages the District's network.

---

- 
2. Develop and adopt a comprehensive written IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

The Director should ensure that the Administrator:

3. Evaluates all enabled network accounts, disables any deemed unneeded and periodically reviews all network user accounts for necessity.
4. Ensures expiration dates are added to the system for temporary network users with set Board appointments or agreements that expire.
5. Is properly notified when contractors no longer need network access.

The Administrator should:

6. Ensure the BOCES supervisor properly notifies them when BOCES staff no longer need network access.
7. Ensure that administrative permissions are only provided for network user accounts that need the permissions as part of the user's job duties and responsibilities.

# Appendix A: Response From District Officials

**Waterville Central Schools**

WATERVILLE NY 13480



**Phone: 315-841-3900**

Website: [www.watervillecsd.org](http://www.watervillecsd.org)

**Fax: 315-841-3939**

Email: [districtoffice@watervillecsd.org](mailto:districtoffice@watervillecsd.org)

## **Administration**

*Dr. Jennifer Spring • Superintendent of Schools  
Joseph Gugino • Interim School Business Official  
Jennifer Dainotto • Secondary Principal  
Karen Hinderling • Elementary Principal  
Kathleen Hansen • Director of Special Programs  
Lindsay Owens • Assistant Principal*

## **Board of Education**

*Timothy Jones • President  
David Poyer • Vice-President  
Peter Casatelli  
Steve Turner  
Linda Hughes  
Daniel Nichols  
Stephen Stanton*

October 27, 2022

Office of the New York State Comptroller  
Division of Local Government & School Accountability  
PSU - CAP Submission  
110 State Street, 12th Floor  
Albany, NY 12236

**Unit Name:** Waterville Central School District

**Audit Report Title:** Network User Accounts and Information Technology Contingency Planning

**Audit Report Number:** 2022M-111

To Whom It May Concern;

This response letter will also serve as the district's Corrective Action Plan (CAP).

Waterville Central School District had an Instructional Technology audit performed during the 2021-2022 school year. The district would like to thank those involved in the audit for their professional and congenial nature as they conducted our audit. The district was provided with the draft report on October 12th, 2022 and the district agrees with the draft report findings.

While most network attacks occur through email, the district continues to work with the Mohawk Regional Information Center (MORIC) and Oneida-Herkimer-Madison Oneida BOCES (OHM BOCES) to navigate the ever changing cyber threat landscape. The recommendations in this draft audit report will also assist in further strengthening the district's protections and recovery from the cyber threat landscape such as an in-house District Contingency Plan and written procedures for network accounts, etc....

The public report detailed seven (7) recommendations. For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed;

---

381 Madison Street • Waterville, New York 13480

---

# Waterville Central Schools

WATERVILLE NY 13480



Phone: 315-841-3900  
Website: [www.watervillecsd.org](http://www.watervillecsd.org)

Fax: 315-841-3939  
Email: [districtoffice@watervillecsd.org](mailto:districtoffice@watervillecsd.org)

## Administration

*Dr. Jennifer Spring • Superintendent of Schools*  
*Joseph Gugino • Interim School Business Official*  
*Jennifer Dainotto • Secondary Principal*  
*Karen Hinderling • Elementary Principal*  
*Kathleen Hansen • Director of Special Programs*  
*Lindsay Owens • Assistant Principal*

## Board of Education

*Timothy Jones • President*  
*David Poyer • Vice-President*  
*Peter Casatelli*  
*Steve Turner*  
*Linda Hughes*  
*Daniel Nichols*  
*Stephen Stanton*

- **Audit Recommendation One:**

Develop written procedures for granting, changing and disabling user access to the network, including procedures to disable any unneeded accounts when they are no longer needed and to periodically review and monitor all network user accounts for necessity.

**Implementation Plan of Action(s):** While the district currently has procedures in place for granting, changing and disabling user access to the network, including procedures to disable any unneeded accounts when they are no longer needed and to periodically review and monitor all network user accounts for necessity, the district will develop written plans so that they can be followed and/or viewed by any individual involved in the procedure without any question.

**Implementation Date:** By the end of the 2022-2023 school year (June 30th, 2023)

**Person(s) Responsible for Implementation:** Superintendent of Schools, IT Administrator, Assistant Treasurer, Confidential Secretary to the Superintendent

- **Audit Recommendation Two:**

Develop and adopt a comprehensive written IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

**Implementation Plan of Action(s):** The district will receive a template Incident Response Plan from the Mohawk Regional Information Center (MORIC) and will use it to develop a district specific written IT Contingency plan.

**Implementation Date:** By the end of the 2022-2023 school year (June 30th, 2023)

**Person(s) Responsible for Implementation:** Superintendent of Schools and IT Administrator

- **Audit Recommendation Three:**

Evaluates all enabled network accounts, disables any deemed unneeded and periodically reviews all network user accounts for necessity.

**Implementation Plan of Action(s):** Currently, the IT Administrator annually reviews all network accounts for necessity using the employee information provided to them. Through the plan of action presented in audit recommendation one, five and six the IT Administrator will be better notified between periodic reviews so that the IT Administrator can better manage accounts between reviews.

---

381 Madison Street • Waterville, New York 13480

# Waterville Central Schools

WATERVILLE NY 13480



Phone: 315-841-3900  
Website: [www.watervillecsd.org](http://www.watervillecsd.org)

Fax: 315-841-3939  
Email: [districtoffice@watervillecsd.org](mailto:districtoffice@watervillecsd.org)

## Administration

Dr. Jennifer Spring • Superintendent of Schools  
Joseph Gugino • Interim School Business Official  
Jennifer Dainotto • Secondary Principal  
Karen Hinderling • Elementary Principal  
Kathleen Hansen • Director of Special Programs  
Lindsay Owens • Assistant Principal

## Board of Education

Timothy Jones • President  
David Poyer • Vice-President  
Peter Casatelli  
Steve Turner  
Linda Hughes  
Daniel Nichols  
Stephen Stanton

**Implementation Date:** January 1st, 2023

**Person(s) Responsible for Implementation:** IT Administrator

- **Audit Recommendation Four:**

Ensures expiration dates are added to the system for temporary network users with set Board appointments or agreements that expire.

**Implementation Plan of Action(s):** The district implemented a new account provisioning software while the audit was occurring. Once an employee end date is approved by the Board of Education or based on a district agreement the IT Administrator enters the end date in the system and then once the date occurs the provisioning software automatically disables the account.

**Implementation Date:** Completed, April 2022

**Person(s) Responsible for Implementation:** IT Administrator

- **Audit Recommendation Five:**

Properly notify the Administrator when contractors no longer need network access

**Implementation Plan of Action(s):** The IT Director and/or Superintendent of Schools will notify the IT Administrator when a contractor no longer needs network access. Also, during periodic reviews of network accounts the IT Administrator will work with the Superintendent of Schools and Business Official to verify contractor accounts still need access if there are any still active. This process will also be outlined in the written procedures as mentioned in audit recommendation one.

**Implementation Date:** By the end of the 2022-2023 school year (June 30th, 2023)

**Person(s) Responsible for Implementation:** Superintendent of Schools and Business Official, IT Administrator

- **Audit Recommendation Six:**

Ensure the BOCES supervisor properly notifies them when BOCES staff no longer need network access.

**Implementation Plan of Action(s):** The district will create a form to be filled out by BOCES supervisors when an employee needs to be added or removed from the district's network. This form will be returned to the district office for distribution to the proper

---

381 Madison Street • Waterville, New York 13480

---

# Waterville Central Schools

WATERVILLE NY 13480



Phone: 315-841-3900  
Website: [www.watervillecsd.org](http://www.watervillecsd.org)

Fax: 315-841-3939  
Email: [districtoffice@watervillecsd.org](mailto:districtoffice@watervillecsd.org)

## Administration

*Dr. Jennifer Spring • Superintendent of Schools*  
*Joseph Gugino • Interim School Business Official*  
*Jennifer Dainotto • Secondary Principal*  
*Karen Hinderling • Elementary Principal*  
*Kathleen Hansen • Director of Special Programs*  
*Lindsay Owens • Assistant Principal*

## Board of Education

*Timothy Jones • President*  
*David Poyer • Vice-President*  
*Peter Casatelli*  
*Steve Turner*  
*Linda Hughes*  
*Daniel Nichols*  
*Stephen Stanton*

departments which includes IT. IT Support staff will also continue to periodically review network user accounts to verify that the employee still needs network access.

**Implementation Date:** January 1st, 2023

**Person(s) Responsible for Implementation:** Superintendent of Schools and IT Administrator

- **Audit Recommendation Seven:**

Ensure that administrative permissions are only provided for network user accounts that need the permissions as part of the user's job duties and responsibilities.

**Implementation Plan of Action(s):** The implementation Plan of Action outlined in audit recommendation six will also be applied for this audit recommendation. If any elevated administrative permissions for staff who are not involved in the management and support of the network are needed approval will be granted by the Superintendent of Schools and Business Official and/or IT Administrator based on the needs of the situation.

**Implementation Date:** January 1st, 2023

**Person(s) Responsible for Implementation:** Superintendent of Schools and Business Official, IT Administrator

Sincerely,

  
✓ Dr. Jennifer Spring  
Superintendent of Schools

---

381 Madison Street • Waterville, New York 13480

## 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 the District's Director and employees, Administrator, BOCES and MORIC staff and reviewed the District's IT policies and procedures to gain an understanding of the IT environment, specifically those related to granting, modifying and disabling network user accounts and permissions and to determine whether the District had an IT contingency plan.
- We ran a computerized audit script on the District's domain controller on January 21, 2022 to gather network user account information. We then analyzed the reports generated by the script to obtain information about the District's 338 enabled non-student network user accounts, including their permissions, to determine whether they were necessary and appropriate. We identified network user accounts assigned to all contractors, including BOCES and MORIC staff, and any generic accounts that could also be shared or service accounts. We discussed the necessity of these network user accounts with the Director, Administrator and MORIC staff. We also reviewed all enabled network users accounts with administrative permissions to determine whether the permissions were needed and appropriate.

Our audit also examined the adequacy of certain sensitive IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](http://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](mailto:localgov@osc.ny.gov)

[www.osc.state.ny.us/local-government](http://www.osc.state.ny.us/local-government)

Local Government and School Accountability Help Line: (866) 321-8503

---

**SYRACUSE REGIONAL OFFICE** – Rebecca Wilcox, Chief Examiner

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](mailto:Muni-Syracuse@osc.ny.gov)

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



Like us on Facebook at [facebook.com/nyscomptroller](https://facebook.com/nyscomptroller)

Follow us on Twitter [@nyscomptroller](https://twitter.com/nyscomptroller)