REPORT OF EXAMINATION | 2021M-153

Somers Central School District

User Accounts and Software Updates

JULY 2022

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

Contents

Report Highlights

Somers Central School District

Audit Objective

Determine whether Somers Central School District (District) officials established adequate controls over user accounts and software updates to help prevent unauthorized use, access and loss.

Key Findings

District officials did not establish adequate controls over user accounts and software updates to help prevent against unauthorized use, access and loss. Sensitive IT control weaknesses were communicated confidentially to officials. In addition, officials did not:

- Periodically review all network user accounts and permissions to determine whether they were appropriate or needed to be disabled.
  - 58 network user accounts had unnecessary administrative permissions.
  - 111 network user accounts were unneeded and should have been disabled.
- Adopt an adequate comprehensive information technology (IT) contingency plan to minimize the risk of data loss or prevent a serious interruption of services. Consequently, in the event of a system disruption due to a disaster, ransomware attack or other event, employees have insufficient guidance to restore or resume essential operations.

Key Recommendations

- Develop written procedures for managing network user account access.
- Develop and adopt a comprehensive IT contingency plan and communicate it to appropriate officials and employees.

Background

The District is located in Westchester County and is governed by a seven-member Board of Education (Board) responsible for the District's overall governance.

The Superintendent is the chief executive officer and responsible, along with other administrative staff, for day-to-day operations.

The District's Information Technology Director (IT Director) is responsible for ensuring the IT infrastructure is based on industry standard practices and overseeing the IT vendor.

The District contracted with an IT vendor to operate and maintain the District's IT system.

Quick Facts	
Students	2,818
Employees	611
IT Vendor Payments for 2020-21	$510,715
Network User Accounts	
Student	2,875
Nonstudent, Non-generic	988
Generic	153
Total	4,016
Reviewed	4,016

Audit Period

July 1, 2019 – April 22, 2021

We extended our scope forward to June 23, 2021 to complete IT testing.

District officials agreed with our findings and indicated they plan to initiate corrective action.

User Accounts and Software Updates

The District's IT system and data are valuable resources. The District relies on its IT assets for Internet access, email and for maintenance of financial and personnel records, much of which contain personal, private and sensitive information (PPSI).[1] If the IT system is compromised, the results could be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls do not guarantee a computer system's safety, a lack of effective controls significantly increases the risk of unauthorized use, access and loss.

The district should have written procedures for granting, changing and disabling access to the network and computer resources.

How Should District Officials Manage Network User Accounts and Permissions?

User accounts provide access to a district's network and computer resources, and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers to inappropriately use, access and/or delete PPSI on the network. The district should have written procedures for granting, changing and disabling access to the network and computer resources. These procedures should establish who has the authority to grant or change access and allow users to access only what is necessary to complete their job duties and assignments.

Generic user accounts may be needed for certain network services or applications to run properly. However, they should be limited in use, as they are not linked to individual users and, therefore, have reduced accountability. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service help desk account. Officials should also routinely evaluate generic user accounts and disable those that are not related to a current district or system need.

Generally, an administrative account has permissions to monitor and control networks and computers. Users with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes and can add new users and change user passwords and permissions. As a result, officials should limit network administrative permissions to only those users who need them to perform their job duties, responsibilities and assignments.

When users have unneeded network administrative permissions, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems. A user can be deceived into opening a malicious

1 Personal, private and sensitive information (PPSI) is any information where authorized 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.

email attachment, downloading and opening a file from a malicious website or accessing a website programmed to automatically infect the user's computer with malicious software. If the deceived user has administrative permissions, an attacker could use those elevated privileges to cause greater damage than with a lesser-privileged account.

To minimize the risk of unauthorized access, district officials should actively manage network and local user accounts to ensure they are appropriate and still needed. Officials should disable unnecessary or unneeded accounts as soon as there is no longer a need for them.

District Officials Did Not Adequately Manage Network User Accounts and Permissions

District officials did not develop comprehensive written procedures for managing network access that include periodically reviewing user accounts and disabling network accounts when access was no longer needed. The District has written procedures for granting, changing and terminating access rights. However, the procedures do not state the process of adding and disabling user accounts, and who has the authority to do so. As a result, employees do not have clear guidelines on when to add or disable user accounts, which increases the risk that the District could have excess unneeded accounts, compromising system security.

The IT Director stated this occurred because the IT vendor failed to perform his duties as required by the contract terms. The contract states that the IT vendor is responsible for the administration and maintenance of all network user accounts. Due to concerns regarding the IT vendor's performance, the District changed IT vendors as of July 1, 2021. The new vendor will assist District officials with updating their IT procedures. Because these procedures were lacking and the vendor failed to adequately manage network user accounts, we reviewed network user accounts and found the following deficiencies:

Unneeded Nonstudent and Non-generic User Accounts – We reviewed all 988 nonstudent and non-generic network users accounts for inactive user accounts (accounts that had not logged into the network for at least six months before April 22, 2021). We identified 52 employee network user accounts that were for former employees and, therefore, were not needed.

Unneeded Student User Accounts – We reviewed all 2,875 student network user accounts and identified 26 accounts that were unneeded because they were assigned to students no longer enrolled at the District. Some users we reviewed have an active directory account but are not considered as enrolled students because they are BOCES students, may have transferred, or are in pre-kindergarten, homeschooled or in a private school.

Unneeded Generic Accounts – We asked the IT Director about all 153 generic accounts to assess whether they were necessary for District operations and found that 33 were unneeded. These unneeded accounts included test accounts before adding a user to the network, and accounts the technology department used to give to presenters and the library, or to temporarily assign to someone.

Unneeded Administrative Permissions – We found 58 network user accounts had unnecessary administrative permissions for the network. All of these users can change network configuration settings on the network, and they did not need these permissions to perform their normal job duties. The unneeded administrative access was because the previous IT vendor thought they needed the elevated access to run District applications.

Human Resources works directly with the IT vendor to disable network user accounts. However, the IT Director stated she was aware that the previous IT vendor's performance was not acceptable and that is why the District changed IT vendors. The IT Director was not aware of the unneeded accounts or excessive permissions until we brought it to her attention.

Without formal procedures for regularly reviewing enabled user accounts, the District has a greater risk that the unneeded access could be compromised or used for malicious purposes. Unneeded network user accounts should be disabled promptly to decrease the risk of unauthorized access and potential entry points for attackers.

Why Is Contingency Planning Important?

An IT contingency plan is a district's recovery strategy, composed of the procedures and technical measures that enable the recovery of IT operations after an unexpected incident. An unexpected incident could include a software failure caused by a virus or malicious software or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such events.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of the district's operations and IT environment. Proactively anticipating and planning for IT disruptions prepares personnel for the actions they must take in the event of an incident. The goal of an IT contingency plan is to enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

Because IT often supports key business processes, planning specifically for disruptions is a necessary part of contingency planning. A comprehensive IT

The goal of an IT contingency plan is to enable the recovery of a computer system and/or electronic data as quickly and effectively as possible following an unplanned disruption.

contingency plan should focus on strategies for sustaining a 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. Policies and procedures are also critical components and 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 the district, 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
- Details concerning how the plan will be periodically tested.

The District's Contingency Planning Was Inadequate

Although District officials store backups in an offsite location and created a disaster recovery plan (plan) in April 2021, after we engaged this audit, the plan was inadequate and not comprehensive. While the plan discusses ransomware attacks, it does not address the range of threats to the District's IT system. It does not focus on sustaining critical business functions during and after a disruption such as the location to setup after the disruption. The plan does not give specific details of restoration such as what resources are needed to recover in the event of an emergency, and the roles and responsibilities of key personnel. The District has a network report with procedures, but it is not incorporated into the plan. There are no policies or procedures listed in the plan. The plan does not include backup procedures requiring when backups should be tested and documenting whether they were successful.

Consequently, in the event of a disruption, a disaster, phishing[2] or a ransomware attack, employees have insufficient guidance to follow to restore or resume essential operations in a timely manner. Without a comprehensive plan, there is an increased risk that the District could lose important data and suffer a

2 Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.

serious interruption to operations, such as not being able to process checks to pay vendors or employees. The IT Director stated she was aware this plan was lacking after we discussed it with her. The IT Director also told us the previous vendor lacked the resources to assist the District with developing policies and procedures but she would work with the new IT vendor to update the plan.

While the Assistant Superintendent of Business or the Director of Technology Services would be responsible for restoring District data upon a disruption, they were not provided training on this plan. In addition, officials did not test the plan.

Without a comprehensive contingency plan in place that all responsible parties have been trained on and that is periodically tested for effectiveness, District officials have less assurance that employees will react quickly and effectively to maintain business continuity. In addition, without backup procedures and periodic testing of backups, officials cannot ensure the recovery of necessary data to continue operations if a security breach or system malfunction occurs. IT disruptions can occur unexpectedly. As a result, important financial and other data could be lost, or the District could suffer a disruption to operations.

What Do We Recommend?

District officials should:

1. Develop adequate written procedures for managing network access that include periodically reviewing user access and disabling user accounts when access is no longer needed.
2. Ensure administrative permissions are granted only to network users whose job responsibilities require them to have such permissions.
3. Develop, adopt and test a comprehensive IT contingency plan that includes detailed guidance for continuing operations, key personnel and procedures for recovery of IT operations.

Appendix A: Response From District Officials

Forward in Excellence

SCSD
SOMERS CENTRAL SCHOOL DISTRICT

Dr. Raymond H. Blanch
Superintendent of Schools

May 31, 2022

Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Re: Response to draft findings of the audit report titled User Accounts and Software Updates – Report of Examination

To the Office of the State Comptroller:

This letter is to acknowledge the receipt of the draft report titled User Accounts and Software Updates: Report of Examination during the audit period of July 1, 2019 to April 22, 2021. The District agrees with the Comptroller's recommendations and will use them to develop clear and detailed written procedures to enhance controls over user accounts and software updates.

During the audit period, the District's planning was already underway to address the findings as identified in the audit report and will be preparing the Corrective Action Plan that will detail the system improvements. In addition, the District continues the transitioning of its IT operations to new staffing and will work to improve our IT policies and practices to provide all users with a secure and stable network environment.

Lastly, the District would like to thank the Office of State Comptroller for the professionalism their staff showcased during the audit process.

Respectfully,

Dr. Raymond H. Blanch
Superintendent

RHB/nc

District Administration
250 Route 202, Somers, NY 10589 • PO Box 620, Lincolndale, NY 10540
Phone 914.277.2400 • Fax 914.277.2409 • www.somersschools.org

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, employees and the IT vendor to gain an understanding of the District's IT operations and reviewed IT-related policies to gain an understanding of the IT environment, including those for user accounts and software updates.
- We used a computerized audit script to examine the District's domain controller on April 22, 2021.[3] We then analyzed the report to determine whether all users were currently employed by or enrolled in the District. We analyzed all accounts not recently used such as employee accounts, generic accounts and student accounts. We then reviewed network user accounts and relevant security settings configured on the District's network.
- We used our professional judgment to select a sample of six District computers out of 30 that had access to personal, private, and/or sensitive information. We ran a computerized audit script on each of the six selected computers to analyze reports generated by the script, to identify weaknesses in local user accounts and software.
- We obtained the disaster recovery plan from District officials and reviewed the plan to determine whether it was recently updated, met best practices, distributed, and periodically tested to ensure critical issues are identified.

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

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

3 The domain controller is the main server computer in the domain (network) that centrally manages all computers within the domain. It is responsible for allowing users to access network resources.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-1(3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Repor*t, which you received with the draft audit report. We encourage the Board to make the CAP available for public review in the Clerk's office.

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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties

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