REPORT OF EXAMINATION | 2019M-208

Sackets Harbor Central School District

Information Technology

JANUARY 2020

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

Contents

Report Highlights

Sackets Harbor Central School District

Audit Objective

Determine whether the District's network was adequately secure to protect the student management system (SMS) against unauthorized use, access and loss.

Key Findings

District officials did not:

- Establish written procedures for password management, wireless security, remote access and managing user access rights.
- Disable unneeded network user accounts and adequately restrict user permissions to the network and user computers based on job duties.
- Develop a written disaster recovery plan.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive procedures over password management, wireless security and remote access.
- Develop procedures for adding, removing and modifying user access rights to the network and user computers.
- Evaluate user accounts and permissions and ensure unneeded user accounts are disabled and unnecessary permissions are removed.
- Develop a disaster recovery plan.

District officials agreed with our recommendations and indicated they had either already taken, or planned to take, corrective action.

Background

Sackets Harbor Central School District (District) has a single K-12 building and serves the Towns of Adams, Henderson and Hounsfield in Jefferson County.

The District is governed by a five-member Board of Education (Board) that 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.

Quick Facts	
Employees	96
Student Enrollment	436
Desktop, Laptop and Tablet Computers	723
Total Network User Accounts	670
Nonstudent Network User Accounts	193

Audit Period

July 1, 2017 – July 23, 2019

Information Technology

The District relies on its information technology (IT) assets for Internet access, email and maintaining student management system (SMS) records that may involve personal, private and sensitive information (PPSI).[1] The District contracts with the Mohawk Regional Information Center (MORIC) to provide the following IT-related services: network technical support; SMS training, support and management; Internet filtering; antivirus protection; backups; and firewall/intrusion detection. The District's technology coordinator is the network administrator and is responsible for overseeing the general computer system operations.

What Policies and Procedures Should the Board Adopt to Safeguard District IT Assets and Data?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board must establish security policies for all IT assets and information, disseminate the policies to officials and staff, and ensure that officials monitor and enforce the policies.

The board should adopt IT policies that include but are not limited to:

- Acceptable Computer Use − This policy should describe what constitutes appropriate and inappropriate use of IT resources and specific consequences for violations.
- Password Security – This policy should address password complexity, length, age requirements and the number of failed log-on attempts the system will allow.
- Wireless Security – This policy should specify the conditions that wireless devices must satisfy to connect to the district's network.
- Remote Access[2] – This policy should address who is authorized to have remote access, the rules and requirements for connecting remotely and the approval process for granting access.

The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring policy compliance.

1 PPSI is any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

2 Remote access is when a user is allowed to access the school district's network from an off-site location.

The Board and Officials Did Not Establish Adequate IT Security Policies and Procedures

While the Board adopted a comprehensive acceptable use policy, and recently revised IT security policies in April 2019 that provide high-level guidance on issues such as password management and remote access, it has not adopted a policy for wireless security. In addition, the Board's policies provide that the Superintendent or her designee will implement the procedures needed to achieve the policy objectives, but no one has developed written procedures to address these areas of IT operations.

While IT policies and procedures do not guarantee the safety of the District's computer system or the electronic information contained therein, the lack of policies and procedures significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Without comprehensive policies and procedures that explicitly convey the appropriate use of the District's computer equipment and practices to safeguard data, officials cannot ensure employees are aware of their responsibilities.

Why Should the District Manage User Accounts and User Permissions?

User accounts provide access to the district's network and user computers and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network and SMS.

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

Generally, a designated administrator has oversight and control of a network and user computers with the ability to add new users and change users' access 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. The compromise of an account with administrative permissions allows greater damage than with a lesser-privileged account because these accounts have full control over the network or user computer. Therefore, administrative permissions should only be given to those employees who need those access rights to perform their job duties.

A district should have written procedures for granting, changing and revoking access rights to the network. Also, officials should periodically monitor user permissions to ensure that employees have access to only those areas or data that they need for their job functions.

Officials Did Not Adequately Manage User Accounts and Permissions

District officials did not adequately manage user accounts and permissions for the District's network, user computers and SMS servers. As a result, the District had unneeded network accounts that had not been disabled. Additionally, some District employees had excessive administrative rights to the network and user computers.

The District's technology coordinator manages and maintains the District's network, and adds, removes and modifies user access rights to the network and user computers. We examined 193 nonstudent-enabled network user accounts and found 39 network user accounts (20 percent) that were unneeded and could be disabled. This includes 35 generic accounts[3] and four user accounts belonging to former employees. After our inquiry, the technology coordinator disabled nine accounts. While the technology coordinator agreed that the other 30 accounts were likely unnecessary, he requested time to review the contents prior to disabling these accounts.

Additionally, we reviewed 19 network user accounts that had administrative permissions to the District's network and eight network user accounts with administrative rights to 10 user computers[4] to determine whether the permission granted was necessary and in accordance with job duties. We found:

- Seven user accounts had unnecessary administrative permissions to the District's network. Five of these accounts were generic accounts and were not associated with a unique user. After our inquiry, District officials told us they revoked administrative permissions for two of the generic accounts and disabled the other three generic accounts. The remaining two accounts belonged to a former employee and current employee who no longer needed administrative permissions. The technology coordinator told us he planned to disable these accounts, but had not done this as of the end of our onsite fieldwork.
- Two network user accounts had unnecessary local administrative permissions to the 10 user computers we tested.

District officials did not have written procedures for granting, changing and revoking access rights to the District's network and user computers. In addition, officials did not regularly review user accounts to ensure they had appropriate user permissions and were unaware certain users were granted unnecessary administrative privileges.

3 Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for classroom instructional purposes or to scan student tests. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled if necessary.

4 Refer to Appendix C for further information on our sample selection.

Because the District's network has unneeded active user accounts, there is a greater risk that these accounts could be used as entry points for attackers to access PPSI and compromise IT resources. In addition, when employees have inappropriate administrative privileges within the network or user computers, they could make unauthorized changes that might not be detected. Also, the compromise of an account with administrative permissions could cause greater damage than with a lesser-privileged account because these accounts have full control over the network or user computer.

Why Should the District Have a Disaster Recovery Plan?

To minimize the risk of data loss and suffering a serious interruption of services, district officials should establish a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the district's IT system and data, including its SMS application and any PPSI contained therein.

Typically, a plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. It should also reference how the district should backup its computer systems. A backup is a copy of data files and software programs made to replace original versions if there is loss or damage to the original. Backup data should be stored at a secure offsite location, encrypted and routinely tested to ensure its integrity. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

The District Did Not Have a Disaster Recovery Plan

The Board recently adopted a revised IT security policy assigning the Superintendent, or her designee, the duty to develop an IT disaster recovery plan to ensure the protection of critical IT services in the event of any sudden, catastrophic event.

District officials told us that the network and SMS are backed up regularly and are stored offsite at the MORIC. While the MORIC has developed and implemented a disaster recovery system to aid the District in recovering its data in the event of a disaster, District officials have not developed and implemented a written plan as of the end of fieldwork.

Without a formal written plan, responsible parties may not be aware of steps they should take to resume operations in the event of a disaster or ransomware attack.[5]

5 Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until payment is made.

What Do We Recommend?

The Board should:

1. Adopt a wireless security policy.

The Superintendent should:

2. Ensure written IT procedures are established for password management, remote access and wireless security.
3. Ensure written IT procedures are established to address adding, removing and modifying user access rights to the network and user computers.
4. Develop a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

The technology coordinator should:

5. Evaluate all existing network user accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.
6. Assess user permissions for all users on the network and user computers and remove excessive user permissions for those users who do not need that level of access to perform their job duties.

Appendix A: Response From District Officials

Jennifer L. Gaffney, *Superintendent*
Amy Fiedler-Horack, *Principal*
Julie Gayne, *Treasurer*
Sheri Rose, *District Clerk*

Board of Education
Dale R. Phillips, *President*
Angela A. Green , *Vice President*
Christine M. Allen
David W. Altieri
Christine L. Wheeler

Sackets Harbor Central School District
215 South Broad Street
P.O. Box 290
Sackets Harbor, New York 13685
Phone: 315.646.3575 Fax: 315.646.1038

January 3, 2020

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building
333 E. Washington Street, Room 409
Syracuse, New York 13202

To Whom It May Concern:

This letter shall serve as notice that we are in receipt of the Draft Sackets Harbor Central School District Information Technology Report of Examination for the period covered: July 1, 2017-July 23, 2019. Please accept this letter as the Sackets Harbor Central School District's Audit Response and Corrective Action Plan as a result of the School District's recent Comptroller's Audit.

After a close review of the findings, and recommendations, Sackets Harbor Central School District does not dispute the findings of the report. Rather, we applaud the thorough examination of our systems and will implement a corrective action plan to address the areas in need of attention and improvement. The District is thankful for the opportunity to receive valuable feedback to improve our policies and practices related to information security and privacy measures. This audit was particularly timely given the onset of New York State Education Law Section 2-D which aims to increase information security and privacy measures to safeguard Personally Identifiable Information (PII) of students and school personnel. Our District was able to make many necessary compliance changes ahead of this legislation.

Corrective Action Plan

Audit Recommendation 1: Adopt a wireless security policy.

Implementation Plan of Action(s): The District has recently updated our Board Policy Manual. The Manual now includes a number of policies which address wireless security including #5675-Data Networks and Security Access; #6410 - Staff Acceptable Use Policy; and #6411- Use of Email in the District. These policies describe what constitutes appropriate and inappropriate use

of IT resources and consequences for violations. The District recognizes that none of these policies specify the conditions that wireless devices must satisfy to connect to the District's network. Therefore, Policy #5674 entitled Data Networks and Security Access will be updated and written procedures will be developed to detail the conditions that wireless devices must satisfy to connect to the District's network. Furthermore, Ed Law 2-D is requiring school districts to comply with new requirements related to data security and privacy. We anticipate new policies on related topics to be released in the near future for our District's consideration.

Implementation Date: January 2020

Person Responsible for Implementation: The Sackets Harbor Central School District Board of Education and Superintendent are responsible for developing, modifying and/or adopting policy.

Audit Recommendation 2: Ensure written IT procedures are established for password management, remote access, and wireless security.

Implementation Plan of Action(s): The District has developed procedures for password management to address District Policy #5674. These written procedures include the following required specifications: complexity, length, age requirements and the number of failed log-on attempts. The procedures will also indicate the plan for staff training on the topic of password management.

The District has a policy addressing data network and security access (Policy #5674) which gives the superintendent authorization to determine how and who should have remote access and to develop written agreements with remote access users. As part of our procedures, we have also developed written guidance for granting remote access which includes a written agreement for remote access users.

The District has also developed written procedures detailing the conditions that wireless devices must satisfy to connect to the District's network. All of our updated procedures have been disseminated with the necessary stakeholders.

Implementation Date: Fall 2019

Person Responsible for Implementation: The Principal/Director of Technology and Technology Coordinator are responsible for developing and administering the procedures in accordance with District policy.

Audit Recommendation 3: Evaluate all existing network user accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness; Assess user permissions for all users on the network and user computers and remove excessive user permissions for those users who do not need that level of access to perform their job duties; and ensure written IT procedures are established to address adding, removing, and modifying user access rights to the network and user computers.

Implementation Plan of Action(s): The corrective action plan for these related recommendations involved several responses. First, the District immediately evaluated existing user accounts and disabled any deemed unnecessary. We also immediately assessed user permissions for all users and removed excessive user permissions. The District then developed written IT procedures to address adding, removing, and modifying user access rights to the network and user computers. These written procedures are in the form of a guiding document detailing the user rights necessary for each position within the District. This will ensure that each employee gets only the rights necessary to carry out the functions of his/her job and nothing more. Secondly, the District has developed a clearly articulated and sequential process for onboarding/registering and off-boarding/deregistering employees and students in checklist form which requires administrative approval for adding rights. Further, the District also turned on the internal Student Management System (SMS) notification feature which communicates to the necessary staff when students are added or deleted from our enrollment. This notification will result in the necessary action to add, remove, or modify student user access rights. The written procedures also indicate that the Technology Coordinator should monitor user permissions two times per year to ensure that employees and students have access to only those areas or data they were approved for.

Implementation Date: Fall 2019

Person Responsible for Implementation: The Superintendent, Technology Coordinator, and Principal/Director of Technology are responsible for ensuring processes for adding, removing, modifying, and approving user access rights that will protect the integrity of our District network.

Audit Recommendation 4: Develop a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Implementation Plan of Action(s): The District recognizes the importance of having plans in place to minimize the risk of data loss and interruption to our operations in the event of a cyber disaster or ransomware attack. The District has relied for many years on the Madison Oneida Regional Information Center's (MORIC's) Disaster Recovery processes as our own. However,

given the increased threats in our cyber environment, the District understands that the need to develop our own individualized plans so that we know the steps we need to take immediately after a cyber event. The District's team has been in the process of developing a Disaster Recovery Plan, inclusive of incident response measures. These plans refer to a scope of actions to be taken during an incident as well as actions to be taken after an incident occurs to minimize the impact of an unexpected event, recover from it, and return to the normal production level as soon as possible.

Implementation Date: January 2019

Person Responsible for Implementation: Superintendent and her designees are responsible for writing, testing, and updating the disaster recovery plan.

In closing, I would like to thank the field staff of the Comptroller's Office for their professionalism and assistance throughout the review. If you have any questions regarding our response, you are encouraged to contact me.

Respectfully,

Jennifer L. Gaffney
Superintendent of Schools
(315) 646-3575
jgaffney@sacketspatriots.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 and MORIC personnel and reviewed the District's policy manual to gain an understanding of its IT environment, internal controls and disaster recovery.
- We ran computerized audit scripts and analyzed the reports produced to assess network user accounts, local user accounts, user account permissions and related security settings. We reviewed nonstudent user accounts and compared them to the current employee list to identify inactive and unneeded accounts.
- Using our professional judgment, we ran computerized audit scripts and analyzed reports produced to assess local administrative permissions for 10 computers assigned to eight District users of the SMS to determine whether they were appropriate based upon job function. We chose these individuals because they had access to the SMS and sensitive data.

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.

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 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. 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/localgov/regional_directory.pdf

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

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

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

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

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

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

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

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

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

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

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

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

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