New York State Comptroller
THOMAS P. DiNAPOLI

OnTECH Charter High School

Information Technology

2023M-171 | March 2024

Division of Local Government and School Accountability

Contents

Report Highlights

OnTECH Charter High School

Audit Objective

Determine whether OnTECH Charter High School (School) officials ensured information technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

School officials did not ensure IT systems were adequately secured and protected against unauthorized use, access and loss. In addition to sensitive IT control weaknesses that were communicated confidentially to officials, the Board of Trustees (Board) and officials did not:

- Adequately manage user accounts and permissions. As a result, the six computers tested had unneeded user accounts and unnecessary administrative permissions.
- Monitor Internet usage for compliance with the School's Acceptable Use Policy (AUP). As a result, there is an increased the risk of School computers being exposed to malicious software.
- Develop and adopt an IT contingency plan and provide staff with IT security awareness training. As a result, the School has an increased risk that its IT systems, including their hardware, software and data containing personal, private and sensitive information (PPSI), may be exposed, damaged or lost.

Key Recommendations

- Develop and enforce written procedures for managing user accounts.
- Provide security awareness training and ensure staff comply with the AUP.
- Develop, adopt, distribute, and periodically update and test a comprehensive IT contingency plan.

School officials agreed with our recommendations and indicated they have initiated or plan to initiate corrective action.

Audit Period

July 1, 2021 – June 21, 2023

Background

The School is located in the City of Syracuse in Onondaga County. The New York State Board of Regents approved the School's charter in July 2018. The five-member Board is responsible for the general management and control of financial and educational affairs.

The Head of School is the chief executive officer and is responsible, along with administrative staff, for the School's day-to-day management under the Board's direction. The Chief Financial Officer (CFO) and a full-time teacher, who serves as the Data and Technology Coordinator (Technology Coordinator), are responsible for overseeing the School's IT operations.

Quick Facts	
Employees	44
Computers	Approximately 300
Students	264

Information Technology

The School relies on its IT systems for conducting day-to-day business, student information system, email and Internet access. IT system users access files that, in some cases, may contain PPSI.[1] If an IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and rebuild. While effective controls do not guarantee an IT system's safety, a lack of effective controls significantly increases the risk of unauthorized use, access and loss. School employees generally use individually configured and managed computers.

How Should Officials Manage User Accounts and Permissions?

To help ensure IT systems are adequately secured and protected against unauthorized use, access and loss, school officials should restrict each user's account access to only what is necessary to complete job duties and responsibilities. User accounts provide access to computer resources and applications for end users and processes, and should be actively managed, including their creation, use and dormancy. School officials should periodically review user account access and permissions to ensure access is appropriate and properly limited based on each user's current and assigned roles and responsibilities. When user accounts are no longer needed, they should be disabled as soon as they are no longer needed. A board and officials should develop and adopt written policies and procedures to help guide system administrators in properly granting, changing and revoking user account access to computers. Officials should also periodically review active user accounts and disable unneeded accounts.

A user account with administrative permissions generally has the ability to add new users and change users' passwords and permissions, and can be used to make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, user accounts with administrative permissions may be accessed to run programs with the same elevated permissions. For example, if malicious software infected a computer, it could run at a higher privilege under a user account accessible on or through that computer with administrative permissions, which could result in a greater risk of computer compromise and/or data loss. Officials should limit user account administrative permissions to those users and processes who need them to complete their job duties and functions.

[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 individuals or entities.

Officials Did Not Adequately Manage User Accounts and Permissions

Officials did not adequately manage user accounts and permissions and periodically review them for appropriateness. As a result, there were unneeded student user accounts and administrative permissions were unnecessarily assigned to School staff. We examined 10 enabled local user accounts (four student accounts and six nonstudent accounts) on six computers,[2] and determined that the four student accounts were not needed because the computers were assigned to staff and not used by students. The Technology Coordinator told us that student accounts were created on staff computers in case the computer was used by or reassigned to a student. However, these student accounts were not accessed in at least six months, including one account that was not accessed in over four years. Therefore, the Technology Coordinator should have disabled these four student accounts to decrease the risk of unauthorized use, access and loss of data. In the event a computer is reassigned to a student in the future, the Technology Coordinator could re-enable the student account when it is needed.

…[T]here were unneeded student user accounts and administrative permissions were unnecessarily assigned to School staff.

Furthermore, the six nonstudent user accounts on six computers had unnecessary administrative permissions. The Technology Coordinator explained that these accounts were given administrative access so staff members were not impeded from completing their assigned job duties and tasks. However, according to the School's AUP, staff are not allowed to make changes to computer configurations (e.g., installing software, modifying applications) without Technology Department approval. Additionally, to help mitigate the risk of unauthorized use, access and loss of data, users who need administrative permissions to fulfill their assigned job duties and responsibilities should also be assigned and use a lesser-privileged user account for routine work when administrative permissions are not needed. The six employees assigned these six computers did not have secondary lesser-privileged user accounts to use when fulfilling their regular job responsibilities.

The School had an increased risk of unauthorized use, access and loss due to unneeded user accounts and user accounts with unnecessary administrative permissions, which existed because officials did not ensure each user's account access was based on their job duties and responsibilities. In addition, the Board and officials did not develop and adopt written policies and procedures for granting, changing, revoking and periodically reviewing user access and administrative permissions. Misuse of administrative permissions is a method often used by attackers to compromise or disrupt IT systems.

[2] See Appendix B for sampling methodology.

How Should Officials Monitor Employees' Internet Use and Compliance With the AUP?

Internet browsing increases the likelihood of computers being exposed to malware, which may compromise PPSI. School officials can reduce the risks to PPSI and IT resources by adopting an AUP, limiting personal Internet use and monitoring usage and compliance with the AUP.

An AUP describes what constitutes appropriate and inappropriate use of IT resources, along with expectations concerning personal use of IT equipment (e.g., Internet access). Officials should ensure that the AUP is distributed to and understood by employees and monitor compliance with the AUP. This involves regularly collecting, reviewing and analyzing Internet use activity for indications of inappropriate or unusual activity, and investigating and reporting such activity.

The School established an AUP that defines the Board's expectations for appropriate IT system user behavior and the Board's right to ensure compliance with the AUP through electronic monitoring of computer and Internet use. The AUP allows web browsing only for School purposes and specifically prohibits certain Internet usage. For example, Internet usage related to gaming, shopping or accessing inappropriate material is prohibited.

Internet browsing increases the likelihood of computers being exposed to malware, which may compromise PPSI.

Employees' School Computers Were Used for Personal Internet Use That Did Not Comply With the AUP

We analyzed the Internet usage history data on seven School computers assigned to seven employees whose job duties provided them with access to PPSI.[3] All seven employees' School computers were used to access websites for personal use, such as vacation planning, social media, personal finances, personal email, home security and job searching. School officials did not monitor compliance with the AUP by periodically reviewing computer website history logs for appropriateness and compliance with the AUP.

The CFO said that the AUP did not accurately reflect what is enforced. The Head of School said that she is discussing an update to the AUP with the Board to allow personal Internet use, while prohibiting commercial and explicit use, because the current AUP is unrealistically strict. While an AUP may include incidental personal Internet use, social media and personal email use are typically excluded because these sites can circumvent security measures in place to protect computer systems and data. Additionally, inappropriate sites (e.g., gambling websites) should be prohibited.

[3] See Appendix B for sampling methodology.

Internet browsing can increase the risk of School computers being exposed to malicious software because an employee could unknowingly visit an infected website or download a malicious file from the Internet. As a result, if an employee's user account is compromised, the School's IT systems and PPSI would have a higher risk of exposure to breach, damage, or unauthorized use, access or loss. Furthermore, when actual practices are not in line with the AUP and known violations are not addressed, the School's ability to enforce compliance could be diminished.

Additionally, there was no process to help ensure staff members understood or acknowledged the AUP. The CFO said he did not realize the importance of ensuring the acknowledgment and understanding of users. If users are not aware or do not understand the policy, they may unknowingly violate the AUP.

Why Should Officials Develop and Adopt an IT Contingency Plan and Provide IT Security Awareness Training?

To help minimize the risk of IT system and data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster, school officials should develop and adopt a comprehensive written IT contingency plan. These events can include power outages, software or hardware failures caused by a virus or other type of malicious software (e.g., ransomware), human error, equipment destruction or a natural disaster (e.g., flood, fire). IT contingency planning involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to recover IT systems and data and quickly resume operations in the event of an unplanned disruption.

School officials should periodically test and update the plan, as needed, to evaluate and help ensure its effectiveness in the event of a disruption. Testing and updating IT contingency plans are particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks. These plans should be distributed to key officials to help ensure they understand their roles and responsibilities during and after an unplanned IT disruption and to address changes in IT systems or requirements.

Studies show that human error accounts for a significant share of all cybersecurity breaches. Therefore, to help minimize the risk of a disruption, officials should provide periodic IT security awareness training that explains common security threats and the proper rules of behavior for using the Internet and IT resources, systems and data. The training should communicate related policies and procedures to all IT system users so they understand IT security measures and their roles in safeguarding data and IT assets. For example, the training should cover key security concepts such as the dangers of downloading files and programs from the Internet; the importance of selecting strong passwords;

requirements related to protecting PPSI; and how to respond if a virus or an information security breach is detected.

Officials Did Not Develop and Adopt an IT Contingency Plan or Provide IT Security Awareness Training

The Board and School officials did not develop and adopt an IT contingency plan to describe the procedures and technical measures officials should take to respond to potential IT disruptions. Additionally, School officials did not provide IT security awareness training to ensure employees understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the School's network and IT assets. These are widely accepted and well-known foundational IT security practices. Without a plan and training, the School had an increased risk that its IT systems, including their hardware, software and data containing PPSI, may be exposed, damaged or lost.

Consequently, in the event of a disruption or attack (e.g., ransomware), School officials and employees had no written guidance or training for restoring or resuming essential operations in a timely manner to help minimize damage and recovery costs. Furthermore, there was an increased risk that the School could lose important data and suffer a serious interruption to operations.

Without a plan and training, the School had an increased risk that its IT systems, including their hardware, software and data containing PPSI, may be exposed, damaged or lost.

What Do We Recommend?

The Board and School officials should:

1. Develop, adopt and enforce written policies and procedures for managing user accounts. At a minimum, these procedures should include granting, changing and revoking user account access to School computers, and periodically reviewing user account access and disabling user accounts as soon as access is no longer needed.

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

3. Ensure IT security awareness training is periodically provided to all individuals who use School IT resources.

The CFO and Technology Coordinator should:

4. Review administrative permissions assigned to user accounts and remove unneeded user accounts and excessive user permissions that are not appropriate for their job duties. Users who need administrative permissions to fulfill their assigned job duties and responsibilities should

be assigned a lesser-privileged user account for routine work when administrative permissions are not needed.

5. Monitor employee Internet use on School computers and implement procedures to ensure employees comply with the AUP, including but not limited to ensuring employees understand and acknowledge the AUP.

Appendix A: Response From School Officials

OnTECH
CHARTER HIGH SCHOOL

March 4, 2024

Rebecca Wilcox, Chief of Municipal Audits
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428

Audit Number 2023M-171

Dear Ms. Wilcox:

Thank you for providing us with the findings related to the OnTECH Charter High School Information Technology Audit. We have reviewed the summary findings, and we agree with the key recommendations that school officials should implement to safeguard operational systems and our network.

Additionally, we have already implemented the following safeguards which will be included in our full corrective action plan (CAP):

- 40 of our 44 employees have been issued school-owned [redacted] to replace the previous [redacted] computers so that we can more readily manage user account privileges and monitor computer usage.
- In advance of developing a full CAP and IT contingency plan, we have begun to upgrade cloud-based software licenses to allow local backups to be maintained.
- These initial steps are directed toward better managing user accounts as suggested, configuring accounts in ways that enable better security, and assigning permissions limited to the necessary functions of the user.
- We have implemented web-based IT security training, required for all employees, with a knowledge gap assessment and four courses initially assigned, followed by one to four additional courses per month. Examples of course already assigned are mobile device security, public wifi, using email safely and secure passwords & authentication.

Providing a safe IT environment to students and staff is an important OnTECH Charter High School goal. The findings and recommendations of the draft and final audit reports will be helpful to improving the school's IT systems, and a comprehensive CAP will be submitted shortly. Thank you for providing the report.

Sincerely

Ellen K. Eagen
Head of School

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 Section 2854 of the New York State Education Law, as amended by Chapter 56 of the Laws of 2014. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed School officials and reviewed the School's IT policies and procedures to gain an understanding of the IT environment, the management of user accounts and permissions, and to determine whether the School had an IT contingency plan and provided IT security awareness training.
- We used our professional judgment to select a sample of 10 employees who had access to PPSI as a result of their assigned job duties and responsibilities. Three employees did not have School computers assigned to them. Therefore, we tested seven School-issued computers assigned to these employees.
- We ran a computerized audit script on March 8 and March 9, 2023 on the six computers with enabled local user accounts. We analyzed the results generated by the script to obtain information about the computers' enabled local user accounts, including their permissions, to determine whether the user accounts and permissions were necessary.
- We ran a computerized audit script on March 8 and March 9, 2023 on six computers to export their web history data. We reviewed the web history of the month with the most activity on each of the six computers to evaluate whether the Internet use was in accordance with the AUP. We took and examined screenshots of the web history data for the remaining computer on May 2, 2023 to evaluate whether the Internet use was in accordance with the AUP.

Our audit also examined the adequacy of certain 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 School 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. We encourage the Board to prepare a written corrective action plan (CAP) that addresses the recommendations in this report and forward it to our office within 90 days. 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 School's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/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.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.ny.gov/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

https://www.osc.ny.gov/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