REPORT OF EXAMINATION | 2020M-80

Oneida City School District

Information Technology

OCTOBER 2020

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

Contents

Report Highlights

Oneida City School District

Audit Objective

Determine whether the Oneida City School District's (District) network was adequately secure to protect the student information system (SIS) against unauthorized use, access and loss.

Key Findings

The District's network was not adequately secure to protect the SIS against unauthorized use, access and loss.

- District officials did not adequately manage user accounts or administrative permissions to limit access to assets and data.
- Some District computers were used for personal activity, increasing the likelihood of the District's network being exposed to malicious software.
- A written disaster recovery plan was not made available to us or the Board of Education for review and approval.

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

Key Recommendations

- Review network user accounts and permissions, disable unnecessary accounts and remove excessive permissions.
- Monitor employees' Internet use and enforce the District's acceptable use policy (AUP).
- Ensure that a comprehensive written disaster recovery plan is developed and shared with key District officials.

District officials agreed with our recommendations and indicated they have initiated corrective action.

Background

The District serves the City of Oneida and Towns of Lenox and Lincoln in Madison County and serves the Towns of Vernon, Verona and Vienna in Oneida County.

The District is governed by a seven-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 chief executive officer and is responsible, along with other administrative staff, for day-to-day management.

Quick Facts	
Student Enrollment	1,946
Employees	334
Total Network User Accounts	3,120
Nonstudent Network User Accounts	864

Audit Period

July 1, 2018 – December 3, 2019

Information Technology

The District relies on its IT assets for Internet access, email and maintaining SIS records that may involve personal, private and sensitive information (PPSI).[1] The District contracts with the Mohawk Regional Information Center (MORIC) to provide IT-related services, including network technical support; SIS training, support and management; Internet filtering; and firewall/intrusion detection. The District has a full time Special Programs Administrator (Administrator), a Computer Service/Network Engineer (Network Engineer) and a Computer Support Specialist who provide IT services for the District.

How Should a District Manage User Accounts and Administrative Access?

User accounts provide access to a district's network and user computers and should be actively managed to minimize the risk of misuse. User accounts could be entry points for attackers because they could be used to inappropriately access and view PPSI on the network and the District's SIS. District officials should regularly review enabled network and local user accounts[2] 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 and manipulating security settings. 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.

District policy[3] requires user rights to be limited to only those information system assets and data that are appropriate to the user's job duties. It also requires a periodic review of the roster of users and their assigned access rights. Further, the policy requires staff to make adjustments to reflect any changes in circumstances.

---

1 PPSI is any information where 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.

2 Network user accounts provide access to resources on a network and are managed centrally by a server and/or domain controller. Local user accounts provide access to resources on specific computers and are managed individually on each computer. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. A domain controller is the main server in the domain (network) that controls or manages all computers within the domain.

3 Policy 5301: Purpose, Use and Administration of District Digital Information Systems

Officials Did Not Adequately Manage User Accounts and Administrative Access

The Administrator and Network Engineer manage and maintain the District's network and add, remove and modify user access rights to the network and user computers. We examined 864 nonstudent network accounts and found 164 accounts (19 percent) that were unnecessary and could be disabled. This included 127 individual user accounts, 30 generic accounts, six shared accounts and one individual account belonging to a current employee.[4] Many of the unneeded accounts were for former substitute employees that could have been identified sooner had officials routinely reviewed network users. District officials told us they disabled or deleted 84 of these network user accounts and seven more will be disabled.

District officials told us the remaining 73 network user accounts are needed but did not tell us how they will be used. We question why these network user accounts are needed because they have not been used in over six months. All of these accounts are assigned to individual users and have never been used. Forty-six of these accounts were created over two years ago, including four that were created in 2011 (over eight years from the test date).[5]

We also examined the local user accounts on a sample of 10 computers.[6] We identified 11 local user accounts on nine computers.[7] We found one local user account on one of the computers that District officials said was unneeded. After our inquiry, the Administrator stated she deleted this local user account.

In addition, we reviewed 12 network user accounts with administrative permissions to the network and 21 network user accounts with administrative permission to local user computers; and we reviewed 31 local user accounts that had administrative permissions to the local user computers and two SIS servers. District officials told us that all network and local administrative permissions were needed. While most were reasonable, we question why three network user accounts required administrative permissions to local user computers because the accounts had not been recently used and therefore did not appear necessary to perform job duties. For example, the last log-in time stamps for two of these accounts were December 2015 and December 2016 (over three years from the date of our test). The other account, created in November 2018, has never been used and the individual has another user account without local administrative privileges that was logged into recently.

4 The employee has two network user accounts.

5 October 31, 2019

6 See Appendix B for sample selection

7 One computer did not have a local user account. Two of the computers had two local user accounts.

The Administrator told us that the IT department relies on an online form[8] to add, modify or remove user access rights and privileges. However, she said they have not performed an in-depth review of network account usernames and permissions. Had this been done, the District may have identified the unnecessary user accounts sooner.

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

How Should Officials Limit Personal Activities to Protect IT Assets and Information?

A school district should have a written AUP that defines the procedures for computer, Internet and email use. The AUP should describe appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP. Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for inappropriate or unusual activity and investigating and reporting such activity.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by routinely monitoring Internet usage and configuring web-filtering software to block access to unacceptable websites and limit access to websites that do not comply with the AUP.

The District's AUP, entitled *Purpose, Use and Administration of District Digital Information Systems*, states that the District's computers are to be used for school-related purposes and that personal use should be limited for such purposes as brief communication with family members. Additionally, users may not use District-owned computers to conduct business transactions not related to users' school responsibilities, or to perform work on behalf of any non-school organization. Employees who engage in inappropriate use may have their access rights modified or revoked, or be subject to discipline consistent with the District's Code of Conduct, applicable laws and collective bargaining agreements.

8 Form 5042.1: Oneida City School District Superintendent's Regulation Network Account Authorization and Technology User Agreement

The AUP establishes the District's right to monitor, review and audit each employee's computer and Internet use. Therefore, employees should not expect privacy when using the system. Employees are provided a copy of the AUP on a yearly basis in the employee handbook and are required to sign indicating they have received, read, and will uphold all policies contained within the handbook.

Some District Computers Were Used for Personal Activities

We reviewed the Internet browsing history on 10 employees' computers. We selected these employees because their job duties required them to regularly access or have access to PPSI. We found personal Internet use on three computers such as shopping, banking, online bill paying, social media use and web searches for non-District related subjects. One browser history showed more personal use than the others' including post-secondary education and business-related activities not associated with District operations.

All three employees with personal Internet usage signed a form indicating they received, read and would uphold the policies contained in the employee handbook, which included the AUP. Additionally, all three employees' job duties included routinely accessing PPSI.

Although officials told us they use web-filtering software and that the MORIC monitors its firewall, this personal use was not prevented or detected. Internet browsing increases the likelihood of computers being exposed to malicious software that may compromise PPSI. An employee could unknowingly open a malicious email attachment, download a malicious file from the Internet or visit an infected website. As a result, the District's IT assets and PPSI have a higher risk of exposure to damage and PPSI breach, loss, or misuse. Additionally, when employees use District resources for non-District business activities, productivity may be reduced.

We found personal Internet use on three computers such as shopping, banking, online bill paying, social media use and web searches for non-District related subjects.

Why Should a District Have and Share a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of service, district officials should establish a formal written disaster recovery 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 SIS application and PPSI.

Typically, a plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions 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, maintained off-network, encrypted and routinely tested to ensure its integrity. The plan should be periodically tested and updated to ensure key officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

The Board's IT security policy designates the Superintendent, in consultation with the Administrator, as responsible to develop, implement and periodically review procedures and protocols for disaster recovery and information backups.

The District Did Not Provide a Disaster Recovery Plan for Review

District Officials told us that the network and SIS are backed up regularly and backups are stored offsite. Additionally, the Administrator told us the District has a technical disaster recovery plan in a locked location and only she and the Network Engineer know the contents of the plan due to its sensitivity. Therefore, the plan has not been communicated to the Board and other key District officials. In addition, it is unclear what the plan contains because officials refused to provide it for our review. When a disaster recovery plan is not communicated to key officials, responsible parties may not be aware of steps they should take to resume critical operations in the event of a disaster or ransomware[9] attack.

What Do We Recommend?

IT Personnel should:

1. Review network local user accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.
2. Review administrative permissions for all users on the network and user computers and remove excessive user permissions for those users who have access to information system assets and data that are not appropriate for their job duties.
3. Monitor employees' Internet use and enforce the District's AUP.

The Superintendent and Administrator should:

4. Ensure that a comprehensive written disaster recovery plan is developed and shared with key District officials, periodically tested and updated as needed.

9 Ransomware is malicious software that prevents users from accessing their computer systems or electronic data until payment is made.

Appendix A: Response From District Officials

ONEIDA CITY SCHOOL DISTRICT
DISTRICT OFFICE
educate • inspire • empower

August 24, 2020

[redacted]
Office of the State Comptroller
State Office Building
333 E. Washington Street, Room 409
Syracuse, NY 13202

To Whom It May Concern:

This letter is an acknowledgement that the New York State Comptroller's Office conducted an extensive Information Technology Audit of Oneida City School District's Information Technology hardware, software and operating systems including but not limited to internet usage, security and data storage. The Oneida City School District is in receipt of the Draft Audit Report for the period July 1, 2018 – December 3, 2019. Please accept this letter as the District's response to the audit, as pursuant to General Municipal and NYS Education Law.

The Board of Education and administration view this audit as an opportunity to improve operations and governance. Additionally, the audit provides the District with the opportunity to improve our policies and practices related to information security and privacy measures.

We agree with the findings of the audit process and the recommendations provided in the draft report. We will prepare our Corrective Action Plan and will submit it after review and approval by the Board of Education.

The District has already complied with the majority of recommendations in the Audit. As always, the District will continue to implement policies and procedures that provide users, employees and the community a safe, sound and beneficial educational IT environment.

If you have any questions regarding our response, you are encouraged to contact me.

Sincerely,

Mary-Margaret Zehr
Superintendent of Schools

Students Reaching Their FULLEST Potential
565 Sayles Street Oneida, NY 13421 (315)363-2550

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 the District's IT environment and internal controls. We requested to review the District's written disaster recovery plan.
- We analyzed network accounts and settings using a computerized audit script. We compared the 864 nonstudent enabled network user accounts to the active employee list to identify accounts for former employees and/or unauthorized users.
- We used our professional judgment to select a sample of 10 employees assigned to 10 computers. We chose these individuals because they had access to the SIS and sensitive data. We ran computerized audit scripts on those computers to review web histories.
- To determine whether permissions were appropriate, we reviewed 12 network user accounts with administrative permissions to the network and 21 network user accounts with administrative permission to local user computers; and we reviewed 31 local user accounts that had administrative permissions to the local user computers and two SIS servers.

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 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/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

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?title=&body_value=&field_topics_target_id=263206&issued=All

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/sites/default/files/local-government/documents/pdf/2020-05/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?title=&body_value=&field_topics_target_id=263211&issued=All

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

Contact

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

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

www.osc.state.ny.us/local-government

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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief 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