DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-174

East Syracuse Minoa Central School District

Information Technology

JUNE 2021

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

Contents

Report Highlights

East Syracuse Minoa Central School District

Audit Objective

Determine whether East Syracuse Minoa Central School District (District) officials established adequate information technology (IT) controls to ensure employees' personal, private and sensitive information (PPSI) on the financial server was adequately protected from unauthorized access, use and loss.

Key Findings

District officials did not adequately apply established IT controls to ensure PPSI was protected from unauthorized access, use and loss. District officials did not:

- Adequately manage user accounts and permissions.
  - ○ Five individuals left employment between 2015 and 2019 but had active user accounts.
  - ○ Five employees had unnecessary user permissions and 16 active contractor accounts were not needed, including three accounts that were created in 2015 and 2016.
- Ensure contractors signed the acceptable use policy (AUP) forms and retain the forms on file.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Routinely review network user accounts and disable unnecessary accounts in a timely manner.
- Remove financial software user permissions not needed based on job duties.
- Ensure signed AUP forms are retained.

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

Background

The District serves the Towns of Manlius, Cicero, and Dewitt in Onondaga County and the Town of Sullivan in Madison County. The District is governed by a nine-member Board of Education (Board) responsible for the general management and control of financial and educational affairs.

The Superintendent of Schools is the chief executive officer responsible for District administration. The Executive Director of Planning, Development and Technology (IT Director) is responsible for the overall management of the District's IT infrastructure.

Quick Facts	
Network User Accounts	5,058
Non-Student Network User Accounts	990
Desktop, Laptop and Tablet Computers	5,952
Employees	664
Student Enrollment	3,386

Audit Period

July 1, 2019 – August 17, 2020

Information Technology

The District relies on its Information Technology (IT) assets for Internet access, email and maintaining personnel records that contain personal, private and sensitive information (PPSI).[1] This includes the District's financial software, which contains extensive PPSI about employees including Social Security numbers, medical information, retirement registration numbers and bank account numbers. The District has an agreement with the Onondaga-Cortland-Madison Board of Cooperative Educational Services (OCM BOCES) Central New York Regional Information Center (CNYRIC) to provide IT services including offsite backup services, firewall protection services, and housing of the District's servers including the financial server.

The District manages its financial and personnel records with a computerized financial system which resides on a financial server that is connected to the District's network. The District provides users access to the network and systems according to an account matrix. It lists job classifications, as well as user accounts, for the network and various systems that the District maintains. Users of the District's network and systems include employees, students and contractors.[2] The Network Administrator is responsible for granting, modifying and disabling user access to the network and to these systems.

How Should Officials Manage User Accounts and Permissions?

User accounts provide access to network resources and financial software 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 the network and view PPSI on the network and in the financial application.

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

To minimize the risk of unauthorized access, district officials should regularly review enabled user accounts to ensure they are still needed.

In addition, IT managers should set up user accounts with specific permissions needed by each individual to perform their job functions. This ensures access to PPSI is restricted to only those individuals who are authorized to access it. Also, officials should periodically monitor user permissions to ensure that any necessary changes to employees' permissions are made in a timely manner.

[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 (students), third parties or other individuals or entities.

[2] For example, contractors include CNYRIC employees, OCM BOCES employees, children's center staff, the student management system vendor, the energy performance contract vendor and the food service management vendor.

Officials Did Not Adequately Manage User Accounts and Permissions

We reviewed all 990 non-student network user accounts (725 assigned to District employees, 71 assigned to contractors and 194 generic and service accounts)[3] and 15 financial software user accounts assigned to 13 employees. Officials did not adequately manage user accounts and permissions for the District's network and financial software as follows:

Former Employees – As new employees are hired, they are asked to read and sign the acceptable use form. Once the signed form is turned in, a human resources staff member submits a help desk ticket with the employee's name and title for the Network Administrator to create the network user account. Similarly, when an employee leaves the District, a human resources staff member provides the Board-approved resignation document to the Network Administrator, who disables the employee's network user account.

Our review of the 725 enabled network user accounts assigned to employees disclosed that, generally, these users were currently employed by the District. However, we found five enabled network accounts that were assigned to former employees who left District employment from 2015 through 2019 (two teachers, a teaching assistant, substitute and bus driver). After we brought this to the attention of the IT Director, he had the Network Administrator disable these accounts.

Contractors – When contractors need network access and have signed the acceptable use form, the building administrator submits a request to the Network Administrator to create a network user account. When there is no more need for the contractor to have network access, the requesting administrator is supposed to notify the Network Administrator to disable the contractor's account. In addition, the District enters user account access expiration dates in the IT system for some contractors who only need network access for a certain period of time. When these dates are entered, the system automatically ends the user account's access rights as of the specified expiration date.

We reviewed all 71 user accounts assigned to contractors. Based on information provided by the IT Director, 22 of these accounts had expiration dates set in the IT system so the users no longer had network access at the time of our review. The IT Director told us that 16 of the remaining 49 contractor accounts did not need access to the District's network. Three of these accounts, which were created in 2015 and 2016, had never been used to access the District's network and 11 accounts had not been used to access the network during the audit period. The IT Director told us the Network Administrator disabled all 16 user accounts and he will reactivate individual accounts if they are needed in the future.

[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.

Because the District's network had unneeded enabled employee and contractor user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources.

Financial Software User Permissions − We also reviewed user permissions on the District's financial software[4] for 13 employees and found that five employees had unnecessary user permissions that allowed them to access PPSI, which they did not need to fulfill their roles and/or job duties. The unnecessary user permissions included the ability to view, add, delete, and/or modify employees' social security numbers, retirement numbers and the annual health insurance coverage forms.

Although District officials told us that they annually review user permissions in the financial software in conjunction with their independent audit, they did not identify these unnecessary permissions. When users of the financial software have unnecessary user permissions, the District has an increased risk that unauthorized changes could be made to employee information and that employees' PPSI could be used to commit fraud and/or identity theft, and the District would be liable for losses incurred.

How Does an Acceptable Use Policy Help Safeguard PPSI?

An effective process for safeguarding a district's computer assets includes an acceptable use policy (AUP) and associated regulation. An AUP defines the procedures for computer, Internet and email use and holds users accountable for properly using and protecting district resources. The AUP and regulation should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy. District officials should ensure that users sign the AUP forms to indicate they have received the AUP and regulation. Because these documents make users aware and provide an understanding of what is expected of them, these forms should be retained and filed in case they are needed for future reference (e.g., if policy violations are found and the individual disputes they were informed of the requirements).

District Officials Did Not Ensure Contractors Signed an Acceptable Use Form

The Board adopted an AUP and management established accompanying regulations for employee use of the District's computerized information resources which consist of hardware, software, networks and email. The policy and regulation describe what constitutes appropriate and inappropriate use of IT resources and the Board's expectations concerning personal use of IT equipment

[4] See Appendix B for sampling methodology.

and user privacy. The regulation also requires the District to give users a copy of the policy and regulation and to have the employee sign the AUP form before a network account is established. Although District officials told us this policy and regulation pertain to all users and that all employees and contractors should sign the AUP upon employment or engagement with the District, signed forms for contractors were unable to be located.

We selected a sample of 22 employees of the 725 employees who had a user account and requested their signed acceptable use forms. District officials provided signed acceptable use forms for all but one of the employees tested. Even though this employee had not signed the acceptable use form, she was given a user account, which is contrary to the policy. When we brought this to officials' attention, the District disabled her unused network account because the employee did not sign the form.

In addition, of the 71 contractors that had a user account, we selected six and asked to review their signed AUPs. Similarly, even though District policy requires a signed AUP for a network account to be established, District officials could not provide signed forms for the six contractors, which is also contrary to the District's AUP. Officials told us that they collected the forms from the contractors but were unaware where they were located, so we could not verify they were completed. Without signed AUP forms for the contractors, District officials cannot be certain that these users have acknowledged they have read and understood the policy and regulation. This increases the risk that employee PPSI, data, hardware and software may be lost or damaged by inappropriate use or access.

What Do We Recommend?

District Officials should:

1. Review network user accounts on a routine basis and disable network user accounts when they are no longer needed.

2. Assess user permissions for all financial software users and remove excessive permissions for those users who do not need that level of access to perform their job duties.

3. Ensure that contractors sign the acceptable use policy form prior to establishing their user accounts and retain the forms on file.

Appendix A: Response From District Officials

ESM
East Syracuse Minoa
Central School District

District Office
407 Fremont Road
East Syracuse, NY 13057
Fax: 315-434-3020
www.esmschools.org

Dr. Donna J. DeSiato
Superintendent

Phone: 315-434-3012
E-mail: ddesiato@esmschools.org

April 20, 2021

Office of the New York State Comptroller
Rebecca Wilcox, Chief Examiner
State Office Building, Room 409
333 E. Washington St.
Syracuse, NY 13202-1428

Unit Name: East Syracuse Minoa Central School District
Audit Report Title: Information Technology
Audit Report Number: 2020M-174

We are in receipt of the recent audit and confidential IT letter. We agree with the audit's findings. Our response to the audit, will also serve as our Corrective Action Plan (CAP).

We thank the Office of the State Comptroller for the audit recommendations and for the professional manner in which the audit was completed.

For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed:

Audit Recommendation: Review network user accounts on a routine basis and disable network user accounts when they are no longer needed.

- Implementation Plan of Action(s): We will continue our process of disabling accounts as staff members or contractors are no longer associated with the school district. As an additional safeguard, we will compare all accounts annually against active employees and contractors and disable those that are no longer needed.
- Implementation Date: The first review was completed on January 14, 2021, and will continue annually.
- Person responsible for Implementation: Network Administrator.

Audit Recommendation: Assess user permissions for all financial software users and remove excessive permissions for those users who do not need that level of access to perform their job duties.

- Implementation Plan of Action(s): We will compare all accounts annually and review their privileges for appropriateness, and adjust if needed.

- Implementation Date: The first review was completed on April 13, 2020 and will continue annually.
- Person responsible for Implementation: Executive Director of School Business Administration.

Audit Recommendation: Ensure that contractors sign the acceptable use policy form prior to establishing their user accounts and retain the forms on file.

- Implementation Plan of Action(s): Contractors will continue to sign the AUP before they receive a user account. We have digitized all AUPs and are now keeping them in a shared drive so that they are easily accessible.
- Implementation Date: This was completed on November 15, 2020.
- Person responsible for Implementation: Network Administrator.

On behalf of the East Syracuse Minoa Central School District, thank you for the services and support provided for our continued growth and improvement.

Sincerely,

Dr. Donna J. DeSiato
Superintendent of Schools

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 reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of the District's IT operations.
- We examined the District's network user accounts and related settings using a computerized audit script. We reviewed the network accounts and compared them to current employee lists to identify accounts for former employees, unneeded accounts and/or unauthorized users. We reviewed automated network settings to identify any settings that indicated ineffective IT controls.
- We used our professional judgment to select 15 user accounts assigned to 13 employees with access to the financial software. We chose these individuals because they had access to PPSI in the financial software. We reviewed user account permissions for the 15 user accounts and determined whether they were appropriate based on their job duties.
- We compiled a list of the folders and sub-folders from the financial server, along with the related user accounts and groups. We manually reviewed the District's list of shared folders that may contain PPSI data and determined whether users with permissions to those folders required the access to perform their job duties.

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 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