New York State Comptroller
THOMAS P. DiNAPOLI

Young Women's College Prep Charter School of Rochester

Network and Financial Software Access Controls

2022M-147 | January 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Young Women's College Prep Charter School of Rochester

Audit Objective

Determine whether Young Women's College Prep Charter School of Rochester (School) officials ensured network and financial software access controls were adequate.

Key Findings

School officials did not ensure that network and financial software access controls were adequate. As a result, data and personal, private and sensitive information (PPSI) are at greater risk for unauthorized access, misuse or loss.

In addition to sensitive information technology (IT) control weaknesses that were confidentially communicated to officials, we found that:

- Fourteen percent or 10 of the School's network user accounts were not needed. Unneeded network user accounts are additional entry points for someone to inappropriately access the School's network.
- Three network user accounts had unnecessary network administrative permissions.
- Two non-administrator financial software user accounts unnecessarily had full access, including the ability to delete transactions. This provided the ability for users to access and potentially alter data and conceal inappropriate activity.
- The Board of Trustees (Board) did not adopt an adequate written IT contingency plan or provide IT security awareness training.

Key Recommendations

- Properly manage network and financial software user accounts.
- Develop a written IT contingency plan and provide periodic IT security awareness training.

Background

The School is located in the Town of Greece in Monroe County. The New York State Board of Regents approved the School's charter in September 2011.

The School is governed by a nine-member Board that is responsible for managing and controlling the School's financial and educational affairs. The Principal is responsible, along with other administrative staff, for the day-to-day management of the School under the Board's direction.

The IT Systems Administrator (IT Administrator) is the School's only IT employee and is responsible for managing IT operations, including network and financial software access controls. The Director of Operations (Director) is responsible for overseeing the IT Administrator.

Quick Facts

Enabled Network User Accounts	
Individual Nonstudent	58
Service	7
Shared	5
Total	70
Financial Software	
Enabled User Accounts	3

Audit Period

July 1, 2020 – July 12, 2022

School officials agreed with our recommendations and indicated they will initiate corrective action.

Network and Financial Software Access Controls

The School relies on its network and financial software for maintaining financial, student and personnel records and Internet access and email, much of which contain PPSI. 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.

If the School's network or financial software access is compromised or disrupted, the results could range from inconvenience to significant damage and could require extensive effort and resources to evaluate, repair and/or rebuild. While effective network and financial software access controls will not guarantee the safety of these systems, without these controls, the School has an increased risk that its network hardware, financial software and data contained therein, including PPSI, may be exposed, damaged or lost through inappropriate access and use.

How Should Officials Control User Access to the Network and Financial Software?

School officials are responsible for restricting network and financial software user account access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets on the network and in the financial software are secure from unauthorized use, access and/or loss.

To minimize the risk of unauthorized access, misuse and loss, officials should actively manage network and financial software user accounts and permissions, including their creation, use and dormancy. Officials should disable unneeded user accounts as soon as they are no longer needed and regularly monitor them to ensure they are appropriate and authorized.

Network and financial software user accounts provide access to network resources and financial and employee data and should be actively managed to minimize the risk of unauthorized access and misuse. If not properly managed, unneeded user accounts may not be detected and disabled in a timely manner. Also, unneeded user accounts are additional entry points into the school's network, and if accessed by an attacker or a former employee, could be used to inappropriately access the school's network to review and/or remove personal information; make unauthorized changes to school records; or deny legitimate access to the school's network and records.

Officials should limit the use of service and shared accounts, routinely evaluate the need for them and disable those that are not related to a current school or system need. A service account is created for the sole purpose of running a particular network or system service or application (e.g., backups) and are not linked to individual users and, therefore, may have reduced accountability. Shared

user accounts have a username and password that are shared among two or more users. Because shared accounts are not assigned to an individual user, officials may have difficulty managing them and linking suspicious activity to a specific user.

Officials should limit network administrative permissions to user accounts that need them to complete specific job duties and functions. Generally, a network administrative account has permissions to monitor and control a network, connected computers and certain applications, such as adding new users and changing user passwords and permissions. A user with administrative permissions on a network can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

When financial software is used to process transactions and maintain financial records, school officials should establish adequate access controls that provide users access to only those functions that are consistent with their job duties and responsibilities. Officials should ensure that financial software access controls prevent users from being involved in multiple phases of financial transactions, or officials should implement effective compensating controls.

Officials should ensure that deletions and adjustments cannot be made without authorization and that there is a process in place for an independent party to review data entered into and changed in the software. These actions can help maintain the data's integrity.

Officials should ensure the Board-adopted user accounts and access rights policy is adhered to. The policy prohibits the use of shared accounts, restricted user access to only the resources necessary for fulfilling the users' job responsibilities and required that user accounts be deactivated once the user leaves the School.

Officials Did Not Adequately Control User Access to the Network and Financial Software

School officials did not develop written procedures for adding and disabling or removing user accounts and permissions on the network or in the financial software and did not adequately manage network or financial software user account access. As a result, an adequate periodic review of user accounts and permissions was not performed and the School had unneeded user accounts and accounts with unnecessary permissions that were not disabled, removed or monitored.

We examined all 70 enabled network user accounts (58 individual nonstudent accounts, seven service accounts and five shared accounts)[1] and all three enabled financial software user accounts to determine whether the accounts and permissions were necessary and adequately controlled.

Unneeded Service and Shared Network User Accounts – Upon our request, School officials reviewed all five shared and seven service network user accounts and told us that they disabled four shared user accounts and three service network user accounts because they were no longer needed. Three of these accounts had administrative permissions. The disabled user accounts remained enabled much longer than necessary. We found that four of these user accounts were not used in more than four years. The IT Administrator also told us there was an additional unnecessary user account with administrative permissions used to perform service on staff computers that he planned to disable. Although the School's written policy prohibits shared user accounts, one shared account used by a School vendor remained enabled. The IT Administrator could not provide an explanation as to why these accounts were not previously disabled or why he maintained a shared account in violation of policy.

Unneeded Individual Nonstudent Network User Accounts – Upon our request, School officials reviewed all 58 individual nonstudent network user accounts. As a result, the IT Administrator disabled three user accounts (5 percent) that we identified during our audit because they were no longer needed. The disabled accounts included a former School employee, a former individual of an outside organization that worked with the School, and an employee who was on extended medical leave.

These accounts should have been disabled as soon as the individuals left School employment or stopped providing services to the School because unneeded user accounts are additional entry points for attackers. The former employee left School employment in January 2022 and the network user account remained enabled for two months before we identified it. Generally, these accounts were still enabled because the IT Administrator did not have written procedures for disabling accounts. The IT Administrator told us that he disabled the user account permissions for the individual of the outside organization, but mistakenly did not disable the user account.

In total, officials disabled 10 network user accounts (14 percent), including three with administrative permissions, as a result of our audit. Unneeded network user accounts are additional entry points into the School's network and, if accessed by an attacker, could be used to inappropriately access the School's network to view and/or remove personal information; make unauthorized changes to School records; or deny legitimate access to the School's network and records. When

1 There were no student network user accounts.

network user accounts are not monitored, compromised accounts may not be detected in a timely manner.

Unnecessary Network Administrative Permissions – Upon our request, School officials reviewed administrative permissions for all four individual nonstudent network user accounts with administrative permissions and identified three individual nonstudent user accounts with unneeded administrative permissions. The Director and IT Administrator told us that these three user accounts had administrative permissions as a backup in the event the IT Administrator was unavailable for an extended time. Because these permissions were unnecessary to perform their job duties, the IT Administrator told us he removed the permissions from the three user accounts (one of which was also disabled). The IT Administrator told us that the administrative permissions on the fourth user account were potentially unnecessary as the permissions were needed to perform one specific function, but the permissions could probably be removed and the individual could use another network user account when they needed to perform the function.

When user accounts have unneeded network administrative permissions, they could potentially make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method used by attackers to compromise or disrupt the network.

Unnecessary Financial Software Permissions – The Director, bookkeeper and IT Administrator each used a separate user account to access the financial software. We reviewed the permissions for these three user accounts to determine whether they were appropriate and officials implemented adequate corrective action from our prior OSC audit[2] that reported unnecessary full access within the financial software and the need to review audit trail reports. The IT Administrator had permissions necessary to perform his job duties. While individual financial software user accounts were created as recommended by our prior OSC audit, the Director and bookkeeper accounts had full access to all financial software modules, including the ability to change and delete transactions. Certain permissions assigned to the Director and bookkeeper were not necessary to perform their specific job duties and responsibilities.

We examined the School's financial software because officials did not ensure financial software access controls were adequate or establish compensating controls for the software control deficiencies. The software allowed users to make changes and deletions to transaction data, including voided transactions, deletions and adjustments such as to vendor names and disbursement amounts, without approval. As a result, there is an increased risk that unauthorized changes

2 Refer to *Young Women's College Prep Charter School of Rochester – Information Technology (2016M-24)* released May 2016.

to the accounting records could occur and go undetected. The risks associated with these inadequately controlled financial software permissions are increased because the Director signed School disbursement checks up to $3,000 without adequate oversight. Combined, these controls increase the risk of inappropriate School disbursements occurring and not being detected and corrected.

Although the Director said she generates and provides a monthly audit trail report, including a report of void and deleted transactions, to the finance committee for review, officials could not provide documentation supporting that the reports were reviewed. Furthermore, the Board Treasurer (and finance committee chair) told us that he did not receive or review any audit trail reports. Although the Board Treasurer performed an independent review of the bank statements, there was no review of canceled check images because they were not included with the bank statements. Therefore, the Board Treasurer was unable to determine whether the check disbursements were to the appropriate vendors as recorded in the financial software.

We reviewed the sequence of recorded check numbers, void and deleted transactions reports for entries reducing the cash balance, and a sample[3] of check disbursements. We did not identify any questionable activity and found all 65 check disbursements totaling $426,757 were for valid School purposes.

While we did not identify any questionable activity, the ability to alter, add and delete data increases the risk of inappropriate transactions. For example, a user could conceal a theft by issuing an unauthorized check and subsequently deleting the check or changing the vendor name in the financial software. By not reviewing audit trail reports including the void and deleted transaction reports, School officials' ability to detect and properly address inappropriate activity is diminished.

Why Should Officials Adopt a Written IT Contingency Plan?

Officials should develop and adopt an IT contingency plan to enable the recovery of an IT system and/or electronic data, such as the network or financial software and the data contained therein, as quickly and effectively as possible following an unplanned disruption. An unexpected IT disruption could include inadvertent employee action, a power outage, failure caused by a virus or other type of malicious software, equipment destruction or a natural disaster such as a flood or fire. Unplanned service interruptions are inevitable; therefore, it is crucial to plan for such an event. Proactively anticipating and planning for IT disruptions helps prepare personnel for the actions they must take in the event of an incident and could significantly reduce the resulting impact.

3 Refer to Appendix B for further information on our sample selection.

A comprehensive written IT contingency plan is composed of the procedures and technical measures that help enable the recovery of operations and data after an unexpected IT disruption. It should focus on strategies for sustaining a school's critical business processes in the event of a disruption, be distributed to all responsible parties and periodically reviewed, tested and updated.

Typically, an IT contingency plan should address the following key components:

- Roles and responsibilities of key personnel,
- Identifying and prioritizing critical school processes and services,
- Communication protocols with outside parties,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan, and
- Details concerning how the plan will be periodically tested.

Officials Did Not Develop a Comprehensive IT Contingency Plan

School officials did not develop a comprehensive written IT contingency plan. As a result, there is an increased risk that the School could lose important data and suffer a serious interruption to operations, such as not being able to process paychecks or vendor payments.

Although the Board adopted a written disaster recovery plan (as the School's IT contingency plan) in 2016 as recommended in our prior OSC audit, it was not adequately detailed to provide guidance for School officials to continue operations during a disruption. The disaster recovery plan included a brief list of procedures that were not sufficiently detailed to provide guidance to officials and staff in the event of a disruption to adequately recover operations, including network or financial software access, in a timely manner. For example, one procedure was to coordinate temporary installation of financial software, if necessary. However, the procedure did not detail information such as who to coordinate with or what equipment would be used. Furthermore, the disaster recovery plan did not provide information for how users will continue to work during a disruption, such as an alternate worksite to continue School operations in the event the building is no longer operational.

The Director and IT Administrator told us they were unaware that the School's disaster recovery plan was inadequate. Although an IT contingency plan is not a statutory requirement, it is a best practice and essential tool for preparing personnel for the actions they must take in the event of an unexpected IT disruption.

Why Should School Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access to the network and financial software, and misuse or loss of data and PPSI, officials should provide periodic IT security awareness training that explains the rules of behavior for accessing and using the network and financial software and communicates related policies and procedures to all users, including employees and contractors. The training could center on, but not be limited to, emerging cyberattack trends such as information theft, social engineering attacks (methods used to deceive users into revealing confidential or sensitive information), computer viruses and other types of malicious software, all of which may result in PPSI being compromised or denying access to the network or financial software and any data therein.

The training should also cover key security concepts such as the dangers of email, Internet browsing, downloading files and programs from the Internet, requirements related to protecting PPSI on the network or in the financial software and how to respond if a virus or an information security breach is detected.

School Officials Did Not Provide IT Security Awareness Training

School officials did not provide network and financial software users with IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets when accessing the network and financial software. The Director and IT Administrator told us that the IT Administrator sends out periodic emails to all staff with security tips and other information. However, these emails were sent infrequently, such as when the IT Administrator became aware of a new phishing scam. The email did not include any information regarding other risks and the proper behavior when accessing the network and financial software or discuss written School policies or procedures. Furthermore, the emails were only sent to School officials and staff, and not other network users. The Director stated that they previously considered implementing formal IT security awareness training but did not follow through. The Director did not provide any specific explanation as to why they did not formally implement IT security awareness training but indicated they felt the periodic emails were sufficient. The Board did not adopt a policy requiring periodic IT security awareness training.

Without periodic comprehensive IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise the School's network and financial software access. As a result, data and PPSI are at greater risk for unauthorized access, misuse, or loss.

What Do We Recommend?

The Board should:

1. Ensure officials comply with the Board-adopted user accounts and access rights policy.
2. Review and update the School's disaster recovery plan to include essential IT contingency plan components.
3. Adopt a policy requiring periodic IT security awareness training.

The IT Administrator should:

4. Develop written procedures to supplement the Board-adopted policy, including procedures for managing network and financial software user account access controls.
5. Disable unneeded network and financial software user accounts or remove unnecessary permissions in a timely manner, and regularly review and update network and financial software user accounts and permissions.
6. Eliminate shared network user accounts to comply with the School's policy.

School officials should:

7. Consider alternative financial software or implement compensating controls for software deficiencies, such as an independent review of audit trail reports, canceled check images and check number sequences.
8. Provide periodic IT security awareness training to all network and financial software users that reflects current risks identified by the IT community.

Appendix A: Response From School Officials

December 22, 2022

Edward V. Grant, Jr.
Division of Local Government
and School Accountability
Office of the New York State Comptroller
110 State Street
Albany, NY 12236

Dear Mr. Grant,

We have received the draft audit report and have met with your team to review the findings and recommendations. We are in agreement with all recommendations.

The Board and School Officials will work to develop a comprehensive corrective action plan to address the findings and recommendations and will continue to improve our operations.

Sincerely,

Dr. Idonia Owens
Interim Principal

133 Hoover Drive | Rochester, NY 14615 | Phone: 585.254.0320 | Fax: 585.254.0321 | www.youngwomenscollegeprep.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 Section 2854 of the New York State Education Law, as amended by Chapter 56 of the Laws of 2014. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the School's IT and check disbursement policies and procedures and interviewed School officials to gain an understanding of IT operations and controls, specifically those related to network and financial software access.
- We reviewed the prior OSC audit report (2016M-24) released in May 2016 to determine whether officials implemented adequate corrective action.
- We examined network user accounts and permissions using a computerized audit script run on March 28, 2022. We reviewed network user accounts and compared them to current employee lists to identify unused and possibly unneeded network user accounts and permissions.
- We inquired with School officials about possible unneeded network user accounts and permissions.
- We examined financial software user accounts and permissions as of February 17, 2022. We reviewed permissions for the three financial software user accounts to determine whether access was necessary and appropriate based on job duties and responsibilities.
- We reviewed check numbering sequences and followed up on gaps in the numbering sequence (such as voids) because the financial software allowed changes and deletions to data.
- We used our professional judgment to select a sample of 45 check disbursements and used a random number generator to select 20 check disbursements for a total of 65 check disbursements (9 percent) totaling $426,757 of the 890 check disbursements totaling $4.85 million from the period July 1, 2020 through February 10, 2022 and reviewed the supporting documentation (such as purchase order, purchase request form and invoice) to determine whether the disbursement was for a valid School purpose. We also compared the recorded disbursements to canceled check images.
- We reviewed all voided and deleted transactions reducing the cash balance from the period July 1, 2020 through June 10, 2022 as listed on the report generated from the financial software. We compared the deleted transactions to general ledger activity to determine whether the deletions were reasonable, such as for the reversal of a duplicate entry. We reviewed documentation for the voided transactions and discussed with the Director to determine the reason for the void. We also reviewed bank statements to determine whether any voided or deleted checks cleared the bank.

Our audit also examined the adequacy of certain network and financial software access 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 plan of action that addresses the recommendations in this report and forward the plan 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. We encourage the Board to make the CAP available for public review.

Appendix C: Resources and Services

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

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

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

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

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

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

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

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

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

Contact

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

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

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

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties