DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-240

Urban Choice Charter School

Information Technology

JUNE 2020

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

Contents

Report Highlights

Urban Choice Charter School

Audit Objective

Determine whether the Board and School officials ensured information technology (IT) assets were safeguarded.

Key Findings

- A former employee's user account was used to process 510 financial transactions after her resignation.
- School officials did not adopt IT policies or a disaster recovery plan.
- IT users were not provided with IT security awareness training.

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

Key Recommendations

- Immediately disable user accounts of former employees and ensure all IT users have and use their own user accounts when accessing the network and specialized software applications.
- Adopt comprehensive IT policies and procedures and a disaster recovery plan.
- Provide IT users with IT security awareness training.

Background

The Urban Choice Charter School was founded in 2005 and is located in the City of Rochester in Monroe County. The School serves approximately 400 students and has 69 part- and full-time employees.

The School is governed by an eight-member Board of Trustees (Board). The Board is responsible for the general management and control of financial and educational affairs. The Board appointed a chief executive officer to manage the School's day-to-day operations.

The Director of Operations (Director) is the School's chief financial officer and is responsible for maintaining custody of, depositing and disbursing School funds; maintaining the School's financial records; and preparing monthly and annual financial reports for the Board.

The IT Director is the School's only IT employee. He reports to the Director and is responsible for day-to-day IT operations with the assistance of an outside vendor.

Quick Facts	
IT Employees	1
Network Users	121
Number of devices	Approximately 500

Audit Period

July 1, 2018 – November 5, 2019

Information Technology

The Board did not develop a corrective action plan to address significant issues identified in a previous OSC audit report[1] that contained similar findings as this report. As a result, there are continuing deficiencies related to IT that make the School's IT assets and data vulnerable to internal and external threats.

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

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the Board to establish security policies for key IT security issues. School officials should establish computer policies that take into account people, processes and technology and communicate them throughout the School.

New York State Technology Law requires municipalities and other local agencies, including charter schools, to adopt a data breach notification policy that describes actions to be taken to notify affected individuals if personal, private and sensitive information (PPSI)[2] is compromised. Finally, officials should periodically review these policies, update them as needed and designate personnel who are responsible for monitoring policy compliance.

School officials should have an acceptable computer use policy (AUP) that defines procedures for computer, Internet and email use and specific consequences for violations. Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, acceptable use policies or standard security practices. School officials can reduce the risks to PPSI and IT assets by providing network users with IT security awareness training, monitoring Internet usage and developing and implementing procedures to ensure employee compliance with the AUP.

The Board Did Not Adopt Appropriate IT Security Policies and Procedures

Although the School had an AUP, the Board did not adopt any other IT security policies and procedures to address key IT security issues, such as those related

[1] *Urban Choice Charter School, Information Technology (2013M-53)*

[2] PPSI is any information to which unauthorized access, disclosure, modification or destruction – 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.

to data breach notification, data classification, password security, wireless network security, mobile computing and storage devices, online banking, user accounts and permissions, security awareness, sanitization and disposal of IT equipment, and remote access.

Although the School had financial internal control procedures, the procedures did not address IT operations. Consequently, IT assets were at risk for unauthorized, inappropriate and wasteful use, and the School could have incurred a potentially costly disruption of operations and services.

In addition, the School's AUP did not allow personal use of School computers by officials, employees and students. However, officials did not design or implement procedures to monitor compliance with the policy or determine the amount of personal use of School computers.

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

Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, School officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees. The training should center on emerging trends such as information theft, social engineering attacks[3] and computer viruses and other types of malicious software, all of which may result in PPSI compromise. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs, such as secure online banking for users who perform online banking transactions.

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; and how to respond if a virus or an information security breach is detected.

[3] Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

Employees Were Not Provided With IT Security Awareness Training

School officials and employees were not provided with IT security awareness training to help ensure they understood IT security measures designed to safeguard online activity. Officials were unaware of the importance of providing staff with IT security awareness training.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. School officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security.

Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, online banking transactions, School financial data and PPSI could be at a greater risk for unauthorized access, misuse or abuse.

Because School officials did not provide employees with IT security awareness training and did not design or implement procedures to monitor compliance with the AUP,[4] we reviewed the website browsing histories on 13 computers[5] and identified questionable personal use on 12 computers. Users of these computers accessed non-School-related websites used for online shopping, job searches, radio and video streaming, travel information, social media and personal banking (Figure 1). One user, who was not a School employee,[6] accessed these websites more than 3,000 times.

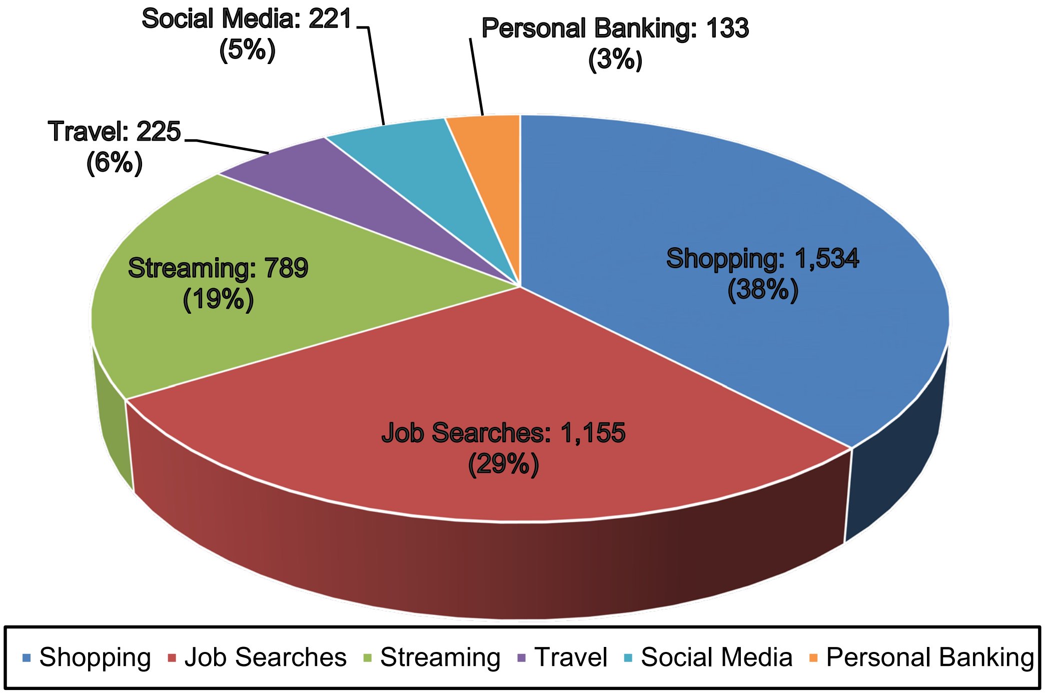
[4] Refer to the What Policies and Procedures Should the Board Adopt To Safeguard IT Assets and Data? and The Board Did Not Adopt Appropriate IT Security Policies and Procedures sections for further information.

[5] Refer to Appendix B for information on our sample selection.

[6] This individual was a nurse who was employed by the Rochester City School District and performed work for the School.

FIGURE 1

Non-School Related Internet Use



Because the School did not provide employees with IT security awareness training, users may have been unaware that accessing these non-School-related websites could compromise PPSI and School IT assets. In addition, because the School did not require officials to monitor Internet use, officials were unaware of this personal and inappropriate computer use.

Internet browsing increases the likelihood of computers being exposed to malicious software that may compromise PPSI or expose the School to ransomware attacks. Allowing personal use of computers increases these risks and can decrease employee productivity. As a result, the School's IT assets and any PPSI they contain have a higher risk of exposure to damage and PPSI breach, loss or misuse.

Why Should Officials Monitor User Accounts and Permissions?

School officials are responsible for restricting user 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 are protected from unauthorized use and/or modification.

User accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating user accounts with specific users. When multiple users are allowed to share user accounts, the School has an increased risk that PPSI could be intentionally or unintentionally changed and/or compromised by unauthorized individuals.

To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When employees leave School employment or transfer to another area, or when user accounts are no longer needed, these user accounts should be disabled in a timely manner. The School should have written procedures for granting, changing and removing user access and permissions to the overall networked computer system and to specific software applications.

Generally, administrative accounts have oversight and control of networks, computers and applications with the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, any program that a user with network or local administrative permissions runs will inherently run with the same permissions. For example, if malicious software (malware) installed itself on a computer, it would run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of network or computer compromise and/or data loss. Officials must limit administrative permissions to those users who need them to complete their job functions.

Officials Did Not Adequately Manage User Accounts and Permissions

Unneeded User Accounts – School officials did not implement comprehensive procedures for managing, limiting, securing and monitoring user access to the School's network and software applications. The IT Director was responsible for adding and deleting users from the network and software applications, such as the accounting and student records systems. When a new employee was hired or an employee left School employment, School personnel sent an informal change request to the IT Director, typically by email, requesting a new account or for an active account to be disabled.

The IT Director told us he reviewed user accounts on a regular basis to determine whether they were still needed and their use was appropriate. However, during our review of 121 enabled network user accounts, we found 26 user accounts (21 percent) that had not been used in at least six months. Of those 26 accounts, the

IT Director told us five were unneeded, should have been disabled and that he would disable them.

We also found that when the former Director of Finance resigned, School officials did not disable her application user account, which had administrative permissions, in the School's accounting system. School officials could not provide an explanation for why her account was not deactivated.

We reviewed the application's audit trail, which contained 4,083 transactions, and found the transactions to be typical of routine School needs. However, we found that the former Director of Finance's application user account was used to process 510 transactions after she left School employment. If users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

<u>Unneeded Generic Accounts</u>[7] – During our review of 121 network user accounts, we found 36 (30 percent) were generic accounts. The IT Director told us that 12 accounts (33 percent) were unneeded, and he would disable them. The IT Director also told us he typically reviewed the list of IT users at the beginning and end of the school year.

Unneeded user accounts can be potential entry points for attackers and could be used to inappropriately access and view personal, private and sensitive information. In addition, when a School has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network, computer and application access.

<u>Unnecessary Administrative Permissions</u> – During our review of the School's network users, we found 15 user accounts that had administrative permissions. However, the IT Director told us he thought he was the only administrator. Because he did not review user permissions for all network accounts on a regular basis, he was unaware of the other user accounts that had administrative permissions.

When users have unneeded administrative permissions to networks, computers and applications, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

A user can be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website, or accessing a website programmed to automatically infect the user's computer with malicious software. If the deceived user has administrative permissions, an attacker could user those elevated privileges to cause greater damage than with a lesser-privileged account.

[7] 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.

Why Should the School Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, officials should establish a formal written disaster recovery plan (plan). This is particularly important given the current and growing threat of ransomware attacks.[8] The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the IT system, financial system and any PPSI contained therein.

Typically, a plan involves analyzing business processes and continuity needs, provides disaster prevention instructions and identifies roles of key individuals and necessary precautions needed to take to maintain or quickly resume operations. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

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. A disaster recovery plan should include data backup procedures, such as ensuring a backup is stored at a secure offsite location, encrypted and periodically tested to ensure its integrity and that it will function as expected.

The School Did Not Have a Disaster Recovery Plan

The Board did not develop a comprehensive written plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster, phishing[9] or a ransomware attack, staff had no guidance to follow to restore or resume essential operations in a timely manner. Without a formal plan, the School has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims.

Although, the School's IT vendor performed regular backups for the school, the backups had never been tested. Without periodic testing of backups, officials cannot ensure they could recover necessary data to continue operations if a security breach or system malfunction occurred.

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

[9] Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.

Why Should School Officials Maintain Accurate and Up-to-Date Hardware and Software Inventory Records?

Computer hardware and software management is of particular importance to larger entities such as schools that have many different users who perform a variety of functions. Typically, schools have several software applications and multiple licenses[10] for each. Maintaining complete and comprehensive hardware and software inventory records is crucial in safeguarding IT assets from loss or theft, tracking the installation of unauthorized and unlicensed software on computers and avoiding fines for unlicensed software installations.

In addition, IT administrators should ensure software is properly licensed. Officials should ensure that software inventory records include all School-owned software installed on computers and the number of copies and version currently in use.

The software inventory record should be used in conjunction with a comprehensive hardware inventory record, which details computer locations and users. These inventory records should be regularly reviewed and matched periodically with all school-owned computers to ensure that all IT assets are accounted for and installed software is properly approved and licensed. Maintaining complete and up-to-date hardware and software inventory records also helps the board develop implement an effective technology replacement plan.

IT Asset Inventory Records Were Inaccurate or Not Maintained

The IT Director maintained a hardware inventory list that contained device names, model and serial numbers, assigned users and locations. However, he updated it at the end of the school year, instead of when a purchase or disposal occurred. For example, during our review of the School's hardware inventory list, we found that 10 users selected for review[11] had 15 computers listed for their use. But, two of the computers (13 percent) were no longer in use. In addition, the IT Director told us he disposed of hardware when he had time and resources, rather than on a regular basis.

Because officials did not ensure that up-to-date hardware inventory records were maintained, the School had an increased risk that IT assets could be lost, stolen or misused. Further, the Board's ability to develop a formalized IT asset replacement plan is hindered.

[10] The purpose of a software license is to grant an end user permission to use one or more copies of a software program in accordance with the US Copyright Act, 17 US Code, Sections 101-810. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Schools must obtain licenses commensurate with the number of copies in use. The penalties for software licensing violations can be severe, exposing the school to legal liability, attorneys' fees and the expense of mandated IT audits.

[11] See supra, note 3.

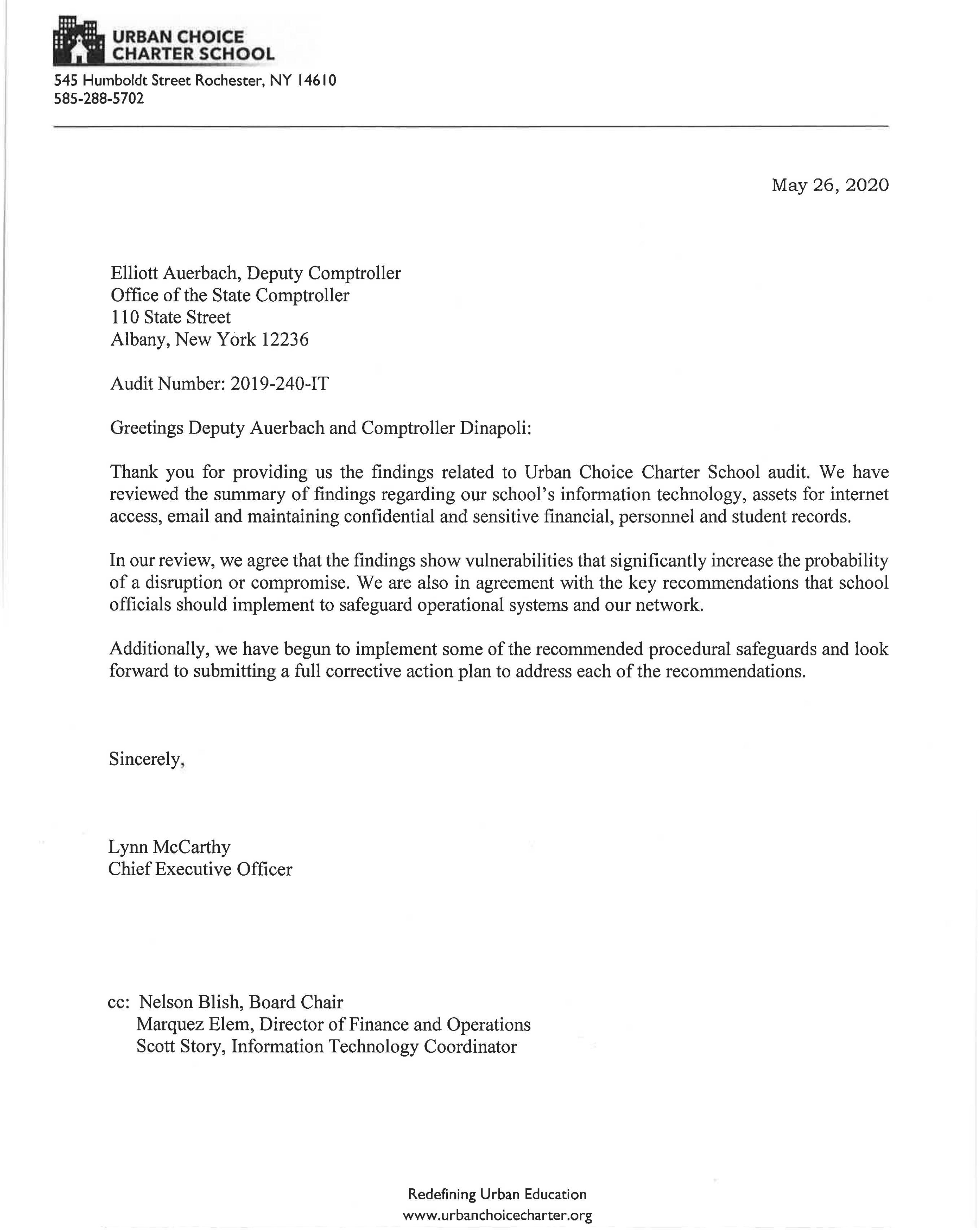
Additionally, School officials did not maintain a software inventory and corresponding software license inventory. Without a complete and comprehensive software inventory, the School is at risk of violating its licensing agreements and allowing unauthorized software on School computers.

What Do We Recommend?

School officials should:

1. Adopt comprehensive IT security policies addressing data breach notification, data classification, password security, wireless network security, mobile computing and storage devices, online banking, user accounts and permissions, IT security awareness training, sanitization and disposal of IT equipment, and remote access.
2. Periodically review and update all IT policies and procedures to reflect changes in technology and the School's computing environment and designate personnel who are responsible for monitoring all IT policies.
3. Provide periodic IT security awareness training to School officials and employees who use IT resources.
4. Implement procedures to monitor network users' computer use for compliance with the School's AUP.
5. Develop comprehensive written procedures for granting, changing and terminating user access to the network and specialized software applications.
6. Immediately disable user accounts of former employees and regularly review and update user accounts for necessity and appropriateness.
7. Ensure all IT users have and use their own network and application user accounts to access the network and specialized software applications, where necessary.
8. Assess user permissions for all network and application user accounts on a regular basis and remove excessive user permissions for those users who do not need that level of access to perform their job duties.
9. Maintain accurate, up-to-date and comprehensive IT hardware and software inventory lists and corresponding software license inventory list.
10. Develop and adopt a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed. Also, ensure data backups are periodically tested.

Appendix A: Response From School Officials



URBAN CHOICE
CHARTER SCHOOL

545 Humboldt Street Rochester, NY 14610
585-288-5702

May 26, 2020

Elliott Auerbach, Deputy Comptroller
Office of the State Comptroller
110 State Street
Albany, New York 12236

Audit Number: 2019-240-IT

Greetings Deputy Auerbach and Comptroller Dinapoli:

Thank you for providing us the findings related to Urban Choice Charter School audit. We have reviewed the summary of findings regarding our school's information technology, assets for internet access, email and maintaining confidential and sensitive financial, personnel and student records.

In our review, we agree that the findings show vulnerabilities that significantly increase the probability of a disruption or compromise. We are also in agreement with the key recommendations that school officials should implement to safeguard operational systems and our network.

Additionally, we have begun to implement some of the recommended procedural safeguards and look forward to submitting a full corrective action plan to address each of the recommendations.

Sincerely,

Lynn McCarthy
Chief Executive Officer

cc: Nelson Blish, Board Chair
Marquez Elem, Director of Finance and Operations
Scott Story, Information Technology Coordinator

Redefining Urban Education
www.urbanchoicecharter.org

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the IT AUP in the School's employee handbook and interviewed School officials to gain an understanding of IT operations.
- We used our professional judgment to select 10 network users, who had access to 13 computers and one server, from the IT hardware inventory and employee lists. We selected these employees based on their access to the School's financial application and potential access to staff and student PPSI. We then reviewed the web browsing history on the 13 computers to determine whether there was any non-School-related activity.
- We scanned the accounting application's audit trail for anomalies, including transactions processed by inappropriate user accounts.

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 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, written corrective action 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/localgov/regional_directory.pdf

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

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

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

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

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

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

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

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

Contact

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

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

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

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

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, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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