

Middle Country Central School District

Review of Information Technology Environment

2019-2020 School Year

September 2020

The Board of Education
Middle Country Central School District
8 43rd Street
Centereach, New York 11720

Board of Education:

We have been retained to function as the internal auditor for the Middle Country Central School District (hereinafter, "the District"). Our responsibility is to assess the internal control system within the District, and to make recommendations to improve upon possible control weaknesses or deficiencies. In doing so, we hope to provide assurance to the District's Board, management, and residents, that the fiscal operations of the District are being handled appropriately and effectively.

BACKGROUND

We performed an initial risk assessment at the District and issued our report dated November 2019 of the results of our review. As part of that risk assessment, we identified the Information Technology area, due to its pervasiveness throughout the District, as an area of risk.

Our objective was to assess the District's internal controls to determine if computer equipment, software, and data are adequately safeguarded. The IT functions in the District are performed under the direct supervision of the Director of Technology, Business and Information Systems. The IT Department is responsible for daily systems support, network access support, as well as backing up and restoring data. To perform our review of the information technology environment, we discussed the roles and responsibilities of District staff and assessed the controls that are in place that relate to information technology, focusing on policies, access controls, and continuity of business operations. In addition, we utilized the Information Technology (IT) Systems Self-Assessment Questionnaire from the Information Technology Guidance produced by the New York State Comptroller's Office, as well as an internally created IT Questionnaire

A. INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

Good governance and accountability require the District's Board to adopt policies and procedures to safeguard District data against unauthorized access, misuse, or abuse. The State Comptroller's Office issued an Information Technology Governance Guide dated March 2012 that includes several recommended policies that school districts should adopt. In addition, school districts are required to adopt a security breach and notification policy as per New York State Technology Law section 208.

District officials are responsible for creating policies and procedures to properly safeguard PPSI against unauthorized access, misuse, or abuse. As noted by the NYS OSC, "a comprehensive PPSI classification policy defines PPSI, explains the entity's reasons for collecting PPSI, and describes specific procedures for the use, access to, storage and

disposal of PPSI involved in normal business activities...[as well as] data classification requirements." Since devices have become more and more mobile, district officials are responsible for implementing policies and procedures that ensure the security of district MCDs. Therefore, the NYS OSC noted that policies should also define which devices are covered (e.g. district-owned or personally-owned), indicate the "procedures for reporting lost or stolen MCDs and storage devices, the process used for gaining approval before connecting new devices to the system and user responsibilities." Districts should have specific care and use guidelines for all district-owned MCDs that are given to staff/students and should require staff/students to sign an agreement regarding care and use of district-owned MCDs.

Lastly, as indicated in the NYS OSC reports on PPSI, a best practice is to have all information, whether in print or electronic form, be classified by assigning a level of risk to various types of information. The risk level assigned should be based on the criticality of the information and the need for appropriate security protocols. Once classified, the data should be labeled in a consistent manner to ensure data confidentiality, integrity, and availability. This is especially important if there is a data breach due to unauthorized system access or theft of equipment.

> **Auditor's Assessment:** The District has several key policies that specify protocols for proper utilization of the District's technology resources which are addressed to all staff and students. We noted that the Board adopted policies that include password management, remote access, encryption, data backups, breach notification, cyberbullying, user accounts, access rights, system administration, record retention, disaster recovery, disposal of equipment containing data, and the protection of personal, private and sensitive information (PPSI). These policies are periodically reviewed and revised as needed to reflect changes in technology or the District's IT environment. Based on our review of the policies in place, the District has taken appropriate measures to implement procedures to reduce the risk that data, hardware, and software systems may be lost or damaged by inappropriate access and use. **No exceptions were noted.**

B. INTERNAL/EXTERNAL SECURITY THREATS

Networks are often connected to the Internet, which means they are connected to users all over the world as well as networks which may not be known. These connections are needed in order to obtain information; however, such accessibility increases the risk of access and attack from unauthorized individuals. Good computing practice is to implement firewalls, which consist of hardware and/or software that enforce boundaries between computer systems and the Internet. Firewalls control network traffic flows, using rule sets which specify which services will pass through the firewall and which services are kept out. Firewalls can also act as effective tracking tools and can perform important logging and auditing functions. As such, the school district network administrator should log and periodically review firewall activities/events.

> **Auditor's Assessment**: The District has installed network monitoring software that collects various statistics from each of the networks and retains the historical usage performance data. It also enables the District to receive warnings of

Cerini & Associates, LLP • 3340 Veterans Memorial Highway • Bohemia, NY 11716
631 582 1600 • 631 582 1714 • www.cerinandassociates.com

potential threats, and alerts if there are variances in performance, such as outages or significant spikes in usage. The software provides information as to who is using the network and what kind of use is occurring (e.g. downloading or possible hacking) thereby helping the District take proactive measures to ensure access to the network will not be compromised. In addition, the District has anti-virus security software, internet filters, and a firewall implemented to prevent viruses and unauthorized use. Lastly, the District has a policy regarding the standards for connecting to the District's network from any external host. Based on the mechanisms and procedures implemented, the District has taken steps to reduce the risk of unauthorized access. **No exceptions were noted.**

C. WIRELESS ACCESS

Wireless networks (Wi-Fi) are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access, and loss of data. However, they are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted into the air. These traveling signals can, potentially, be intercepted and exploited by individuals with malicious intent. Since wireless networks are used as extensions of wired networks, the security problems of a wireless segment can affect an entire network. A wireless environment, therefore, requires certain additional security precautions.

Auditor's Assessment: We noted that the District does not have an open Wi-Fi and requires users to have a District device to use the network. The District has implemented protocols that require users to log on and go through the District's website to gain access to the Internet. Furthermore, the District has implemented filters to restrict access. The District monitors internet activity and is able to limit streaming so that accessibility is not degraded. **No exceptions were noted.**

D. NETWORK ACCESS

The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources. The objectives of limiting access are to ensure that: outsiders (e.g., attackers) cannot gain unauthorized access to systems or data, access to sensitive resources such as operating systems and security software programs are limited to very few individuals who have a valid business need for such access, and employees and contractors are restricted from performing incompatible functions or functions beyond their responsibilities.

School districts should periodically compare the employee master list (as maintained by the personnel or payroll department) to the list of network user accounts to determine if user accounts belong to current employees. A review of all system accounts should be periodically conducted and any account that cannot be associated with an authorized user or application should be disabled.

Auditor's Assessment: Access to the District's network (for both adding, changing, and removing user access) requires notification from Human Resources. All employees receive a network account. For student access, the IT department receives a

list of students from the student services department. Users are assigned to groups and access is permitted based on the access permissions assigned to that group. Access to the District's financial system, nVision, is reviewed on an annual basis by the Business Office, and any changes in access are communicated in writing to the IT department throughout the year. Human Resources will notify the IT department immediately of any terminations. Lastly, we noted that the District utilizes Tools4Ever software which disables the access to the network when a user is deactivated from the student information system or nVision.

While access to the network is restricted, we noted the following:

Issue #1: We noted that the minimum password length is set to six characters.

Risk: Increased risk of unauthorized access as passwords can be more easily guessed.

Level: Moderate

Recommendation: We were informed that the District is in the process of implementing Microsoft's remote password change solution which would permit the District to increase the minimum password length. Due to the pandemic ("COVID-19") and the increased need for Chromebooks to be deployed, the IT staff will be able to fully address this issue once they are able to finish configuring access protocols. We recommend that the District increase the minimum network access password to a minimum of 8 characters once this is complete.

Management's Response: Effective 11/12/2020, the District has increased the minimum password length to 8 characters. Password complexity requirements dictate that they be at least eight characters and meet three of the four following conditions: contain an uppercase character, a lowercase character, a numeric character, and a special character. Passwords may not include names or words that can be easily guessed or identified using a password-cracking mechanism, resets are required every 90 days, and do not allow the last six passwords to be reused.

E. REMOTE ACCESS

Remote access is defined as "the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities" (NIST SP 800 - 114). Many school districts permit users and/or vendors to access district resources remotely for a variety of reasons. It is therefore critical that such access be restricted and secured.

Auditor's Assessment: The District does not permit District users or vendors to remotely access key applications through the District's network. As such, the District minimized the potential exposure to unauthorized remote access. **No exceptions were noted**.

Cerini & Associates, LLP • 3340 Veterans Memorial Highway • Bohemia, NY 11716
631 582 1600 • fax 631 582 1714 • www.cerinandassociates.com

F. WEB FILTERING

Many school district employees require access to the Internet to perform job functions. In addition, teachers and students both utilize the Internet as part of the educational process. School districts often use a web filter to keep students off restricted sites, ensure staff are accessing sites that are needed to conduct legitimate business activities, and ensure that the school's bandwidth is used appropriately. One of the challenges schools face is adequately restricting access to web sites while not impeding business functions or educational activities. With the increase in cybercriminal activity, it is important that access to certain web sites is properly restricted to reduce the threat of unauthorized access.

Web filtering is used to restrict what website users can visit on a device or network. Since the Internet is often utilized when conducting business and educational activities, a school district's asset and user may be exposed to some form of malicious software that could compromise data confidentiality of the user. The web filter classifies websites into categories and the District then restricts access to each category based on the user (i.e. student users, non-teacher faculty, and teachers). Further, the Children's Internet Protection Act (CIPA) specifically requires schools and libraries to block or filter internet access to pictures and material that are "obscene, child pornography, or harmful to minors" on computers that are used by students under 17 years of age.

As the District has had to provide more computers to students in response to COVID-19, internet activity has increased, and the District is more susceptible to significant threats (i.e. malicious software, hackers, etc.) from cybercriminals who are looking to gain unauthorized access to sensitive data. Therefore, it is critical that the District ensures network users are properly using the Internet and pertinent information is safeguarded.

> **Auditor's Assessment**: The District's acceptable use policy provides employees and students with guidelines for IT asset use and security. Specifically, the policy prohibits the use of District computers for non-educational or illegal purposes. In addition, we reviewed a listing of websites that were blocked and noted that the District is compliant with CIPA's Internet access restrictions. **No exceptions were noted.**

G. CYBERSECURITY TRAINING

With the increase in cybercriminal activity, it is critical that school districts ensure that its users are educated in proper Internet use to reduce the risk of security breaches. Providing cybersecurity education to staff and students has become a top priority given the number of breaches that have recently occurred. Cybersecurity education includes understanding what information should be protected, and methods that should be incorporated into everyday access to ensure school district data is protected from unauthorized use, modification, or exploitation.

> **Auditor's Assessment**: The IT staff indicated that they have conducted cybersecurity trainings and subscribe to an IT security awareness training program, KnowBe4, that provides training modules along with simulated phishing attacks on users. In addition, the District subscribes to RIC One through Eastern Suffolk BOCES. The IT staff can then utilize the results of the simulated attacks to determine where additional

training may need to be provided. The trainings cover topics including data privacy and security in an education department which is part of NYS Ed Law 2-d. Subsequent to the review, we noted that the District implemented additional trainings during the Superintendent's conference day. We commend the District's efforts on providing cybersecurity training and increasing user awareness to cybersecurity threats. **No exceptions were noted.**

H. DATA BACKUP & RECOVERY

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. There are four important components to any back-up process:

- Backing up data at regular intervals;
- Verifying the data has been backed up;
- Storing the backup media in a secure, (preferably off-site) location; and
- Verifying the ability to restore the backup data.

Recovery is the process by which an entity can resume business after a disruptive event. The event might be something large, such as a disaster from a major flood, or something small, such as malfunctioning software caused by a computer virus. Recovery procedures need to encompass how employees will communicate, where they will go in the event of a large disruption, and how they will continue to do their jobs. The details can vary greatly depending on the size and scope of the entity and its computerized operations.

Auditor's Assessment: The District systems are backed up and sent to a site at another location within District. The District is in the process of moving all backups to a private secure cloud platform. All services and network switches have Uninterruptible Power Supply (UPS) units which permit the District to safely shut down systems in the event of an emergency or power failure. The District has restored data that is backed up to ensure the backup process is working correctly. Several of the programs utilized by the District are Web-based (for example PowerSchool, IEP Direct and My Learning Plan). As such, the backup and updates occur remotely by the application service provider. In addition, the District's has drafted a comprehensive Disaster Recovery Plan that is updated annually to incorporate any changes in the technology environment. Based on the backup and recovery procedures in place, the District has implemented adequate measures to reduce the risk of delayed or interrupted computer operations and prevent the loss of equipment and data. **No exceptions were noted.**

I. INVENTORY OF IT ASSETS

School districts have and continue to invest a considerable amount of resources in IT assets, which include computers and related equipment. Reliable IT inventory records are critical for protecting these assets from theft, loss or misuse. District officials cannot properly track and protect IT assets if they do not know what IT assets they have and where those assets reside.

District officials should maintain detailed, up-to-date, complete inventory records for all computer equipment located throughout all buildings. The information maintained for each piece of computer equipment should include the following: an asset tag number and

asset description, a serial number, a model number, the date and cost of purchase and the asset's location (i.e., the specific room and building to which the asset has been assigned).

Auditor's Assessment: Through our discussions with the IT staff, the District performed a full inventory of computer equipment during the summer of 2020. The staff utilize Hayes TIPWeb-IT Asset Management program to track the District's computer equipment. **Due to COVID-19 and ensuing safety protocols, we recommend that C&A perform a review when conditions permit to determine whether the District is properly monitoring and safeguarding IT assets.**

We appreciate the cooperation and assistance provided by the District staff during our testing process. We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures.

Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,

Cerini & Associates LLP

Cerini & Associates, LLP
Internal Auditors